ANALYZING THE PERCEIVED PRIVACY OF ELECTRONIC MEDICAL RECORDS IN GOVERNMENT HOSPITALS FOR TANZANIA: A CASE OF DODOMA REGIONAL REFERRAL HOSPITAL

HAPPYNESS HURDSON

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

DEPARTMENT OF MATHEMATICS, INFORMATION AND COMMUNICATION TECHNOLOGY

OF THE OPEN UNIVERSITY OF TANZANIA

2025

CERTIFICATION

The undersigned certifies that she has read and hereby recommends for acceptance by the Open University of Tanzania a proposal entitled **"Analyzing the perceived privacy of electronic medical records in Government Hospitals in Tanzania. A case of Dodoma Regional Referral Hospital".** In partial fulfillment of the requirements for the award of Master of Science in Information Technology Management (MSITM).

…………………………………….

Dr. Juliana Kamaghe

(Supervisor)

……………………………………..

Date

………………..……….……………

Dr. Rogers Bhalalusesa

(Supervisor)

……………………..………………

Date

COPYRIGHT

DECLARATION

I, **Happyness Hurdson**, hereby declare that the work in this paper is my own original work and all sources used or referred to have been documented and recognized. This paper has not been previously submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognized educational institution.”

’

………………………………………..

Signature

………………………..……………

Date

DEDICATION

This work is dedicated to my lovely husband Elisha Thompson Mwankenja, my lovely children Tusajigwe, Glory, Felicia, Bracha, Meira, Everest, and my lovely parents Mr. & Mrs. Hurdson Temu for your prayers, love, support and patience which encouraged me to pursue this course. Thanks for enduring all the pain of missing my company the whole period of study. You mean a lot to me.

ACKNOWLEDGEMENT

Glory be to God almighty, my lord and Saviour Jesus Christ and Holy Spirit for granting me strength, courage, and good health throughout the time of the course, Philippians 4:13” I can do all things through Christ who Strengthen me.”

I would like to express my profound gratitude to my Supervisors, Dr. Juliana Kamaghe and Dr. Rogers Bhalalusesa, for their immense contribution, consistent and unlimited support in tackling my specific problem in the course of this work. Their close follow-up, patience, encouragement, and insights have been the sources of inspiration and success.

Thanks, are also extended to all patients and Dodoma Regional Referral hospital as a government hospital that contributed to the successful completion of this research study. In particular, my sincere gratitude is extended to my lovely parents, Mr. and Mrs. Hurdson Temu to see this achievement, thanks for the prayers, encouragement and patience. Congratulation your dream has been realized.

Moreover, I would not forget to acknowledge the contribution from course lecturers, MSITM students and all member of staffs for the assistance they offered to me during the period of study, which paved the way for the successfully completion of this research work.

I love you all from the bottom of my heart, may Lord Jesus Christ bless you all abundantly. Thank you very much.

ABSTRACT

This study aimed at analyzing the perceived privacy of Electronic Medical Records (EMR) in Government hospitals in Tanzania, a case of Dodoma regional referral hospital. Probability and Non-probability sampling procedures were used through purposive sampling techniques in order to capture information from 210 respondents. Mixed method research design was adopted in conducting this study with both quantitative and qualitative research approaches. Quantitative approach used as the major approach applied, data were collected using Questionnaires, interviews and focus group discussions while qualitative data involves factual and logical interpretation and explanation of the study findings. Data analysis involved descriptive statistics such as frequencies, percentages in order to to draw different tables and charts. In the findings, it is indicated that many of the patients have worries about the privacy of their EMR due to the lack of enough knowledge on how the privacy of their health data is managed, but also there is no clear roles and access level policies for staffs with authorized access to patient's data, staffs do not use a built-in encryption to protect the patient's data privacy. However, due to the existing weaknesses of the firewall system used in the study area, the researcher designs a blockchain framework technology by considering the research objectives, literature reviews, and the results of analyzed collected data from the study. Blockchain technology shows a promising solution to achieve data sharing privacy preservation due to its advantages of immutability, decentralization, transparency and security.

Keywords: *Privacy, Electronic medical records (EMR), Data privacy in Healthcare, Blockchain technology, Government hospital.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AIDS	Acquired immunodeficiency syndrome
DRRH	Dodoma Regional Referral Hospital
e-Health	Electronic health
EHR	Electronic Health Record
EMR	Electronic medical records
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountancy Act
HIT	Health Information Technology
HIV	Human immunodeficiency virus
ICT	Information and communication technology
IT	Information Technology
LISA	Library and Information Science
LISTA	Library, Information Science and Technology
MOH	Ministry of Health
ORLP	Oxford Record Linkage Project
PCI-DSS	Payment Card Industry Data Security Standard
SPSS	Statistical Package for Social Science
USA	United State of America

CHAPTER ONE

INTRODUCTION

1.1 Background Information

Electronic Medical Records (EMR) systems replace paper-based medical records by delivering medical data electronically; also facilitate faster access of health information to relevant health care providers. EMR has become a powerful tool in modern health care delivery. EMRs has greatly improved the safety and quality of health care delivery by increasing access to health information, reducing illegibility and enabling closer overseeing of clinical care processes. In the health care sector, the first attempts at creating digital versions of electronic medical records (EMR) made in 1962, at Oxford Record Linkage Project (ORLP) (Acheson & Evans, 1964).

In an electronic health (e-Health) world, the words EMR and Electronic Health Record (EHR) used very commonly. Most people think that both words EMR and EHR mean the same, but that is not correct. There is confusion between the two words, EMR and EHR and other use the two terms interchangeably, but there is a difference (Charles, 2018).

Maintaining the security, privacy and confidentiality of health data is a global issue. With or without knowing it, people share several types of personal data during their interactions with health care service providers and health facilities. As digital systems now record and store this data, issues relating to privacy, security and confidentiality assume a much greater importance than before. Health data is sensitive and reveal personal details; it is therefore critical to institute measures to avoid unauthorized access and use of it (Sudeep, Sudhanshu & Neeraj, 2020).

The existing EMR system suffersfrom serious shortcomings that affect patients' privacy and safety, and medical practitioners' trust in EMR data (Haux, 2022). The patients' have no power to control over who accesses their private data. There is a lack of a mechanism for evaluating the privacy, security and trustworthiness of patients' medical data (Tertulino, Antunes & Morais, 2024).

Security Concerns in EMR

a. Authentication

Authentication is the process of verifying the identity of a user by using a computer system and can be accomplished using logins/usernames and passwords, digital certificates, smartcards, and biometrics. Authentication only verifies the identity of an individual; it does not define their access (authorization) (Collin, Anish & Douglas, 2020).

b. Confidentiality

According to (Shanholtzer & Ensign, 2025) confidential information can only be provided to the users who are authorized to access, use, and copy the information only if they need information for any productive purpose.

c. Integrity

Integrity refers to the quality of being honest, having strong moral principles, and adhering to ethical standards. It involves being truthful, consistent in actions, and doing the right thing even when no one is watching (Lopez, 2021). Integrity in EMR (Lopez,2022) refers to the accuracy, consistency, and trustworthiness of medical data throughout its lifecycle.

d. Availability

According to the (Vocabulary.com, 2025) availability implies that, electronic system used to collect the data and the security controls used to ensure that the data is accessible and working accurately when the data is required. In other words, the electronic data collection systems, tools and other communication systems must be available and working properly to maintain the security and privacy of data.

1.2 Statement of the Problem

As healthcare systems increase the use of EMRs to streamline patient care, the security and privacy of patient data have become critical concerns. Despite technological advancements in safeguarding these records, patients' perceptions of privacy and trust remain a significant factor influencing their willingness to share personal health information. The effectiveness of EMR systems relies not only on their technical security but also on how secure patients feel about the confidentiality of their sensitive health data.

This research aims to analyze the perceived privacy of EMRs from the perspective of patients, healthcare providers, and other stakeholders. Specifically, the study aims to examine:

- ✓ Patients’ Trust and Concerns: Understanding how patients perceive the privacy of their medical information in an electronic format, including concerns about data breaches, unauthorized access, and misuse.
- ✓ Factors Influencing Perception: Investigating the role of factors such as the level of awareness about data protection, transparency of the healthcare organization’s data practices, and the perceived reliability of the EMR system in shaping privacy concerns.
- ✓ Impact on Health Behavior: Exploring how perceptions of privacy affect patients' willingness to engage with healthcare providers, share sensitive information, and use digital health platforms.

Therefore, the outcome of this research provides an insight on how EMR systems can be improved not only technologically but also from a user trust and perception standpoint. By identifying the factors that shape patient attitudes toward privacy.

1.3 Objectives

1.3.1 General Objective

The main objective of this study is to analyze the perceived privacy of Electronic Medical Records in Government hospitals in Tanzania.

1.3.2 Specific Objectives

i. To determine the EMR privacy techniques used in the study area.

ii. To assess the state of privacy of the EMR system in the study area.

iii. To design an EMR privacy framework for Government hospitals.

iv. To evaluate the designed framework for Government hospitals.

1.4 Research Questions

This study attempts to explore and address the following research questions.

i. What are the techniques used to enhance privacy of EMR in the study area?

ii. What is the state of the privacy of EMR system in the study area?

iii. How can a comprehensive privacy framework be designed for EMRs in government hospitals to enhance patient privacy?

iv. How effective is the proposed EMR privacy framework in improving patient trust?

1.5 Significance of the Research

The main difference for healthcare data as compared with any other industry data is mainly the sensitivity of patient’s healthcare records. Patients want their private data not disclosed without their consent. Therefore, the main significance of this study is to ensure the privacy of the patient’s electronic medical records are protected effectively from unauthorized users like hackers, crackers and information theft.

1.6 Research scope and Limitations

This research aims to analyse the perceived privacy of EMRs in Government hospitals from the perspective of key stakeholders, including patients, healthcare providers, and healthcare administrators. The scope of the study encompasses the following key areas:

- ✓ **Stakeholder Perceptions**: Focus were placed on understanding the perceptions of patients regarding the privacy of their health information in EMRs, as well as healthcare providers' and administrators' views on the associated privacy risks.
- ✓ **Privacy Concerns and Trust**: The study explore specific privacy concerns, including data breaches, unauthorized access, and the potential misuse of EMRs.
- ✓ **Factors Influencing Perception**: The research investigated various factors that shape the perceived privacy of EMRs, including transparency in data management practices, privacy protocols (e.g., encryption, access control).
- ✓ This study is done only on the perceived privacy of the EMR system in Government hospitals for a short period of time. This might not be representative of the whole privacy issues in health services.

Research Limitations:

- ✓ **Geographic Limitations**: The research was limited to specific geographic regions or countries, which may affect the generalizability of the findings to global populations. Cultural, social, and regulatory differences in healthcare systems can impact perceptions of privacy, and the results may not be applicable in all healthcare settings.
- ✓ **Sample Size and Diversity**: The study’s sample may not represent the entire population, particularly with respect to age, socio-economic status, or technological literacy. Patients from certain demographic groups may be overrepresented or underrepresented, potentially skewing the results.

- ✓ **Access to Data**: Obtaining access to EMR systems or patient data might be restricted due to ethical, legal, or technical barriers. This limitation could hinder the ability to comprehensively evaluate the effectiveness of current privacy measures within actual hospital systems.
- ✓ **Time Constraints**: The evolving nature of healthcare data protection and technology may mean that the study's findings quickly become outdated, as new privacy regulations, security technologies, and patient preferences emerge during or after the research period.
- ✓ **Ethical and Legal Constraints**: Ensuring the confidentiality of patient data and obtaining consent for participation could pose challenges, particularly in sensitive healthcare settings. Ethical considerations limit the scope of the data collected and may affect the depth of insights obtained from certain patient groups.

1.7 Organization of the Report

This research report comprises five chapters. The first chapter is general information about the EMR privacy concerns. It will include the statement of the problem, the main objectives, the specific objectives and the research questions of the study. The second chapter is the Literature review; it helps on gathered information through consulting different documentary sources such as publications and files, internet (website), research reports, pamphlets, manuals, progress reports, published and unpublished documents that found relevant with regard to the study objectives.

Chapter three is about research methodology, which shows the insights on how the study will be conducted. It shows the study area, sampling unit and sampling techniques, which used in the study. Chapter four is about findings, results and discussion which show the respondent’s occupation. EMR characteristics, the state of EMR privacy and the EMR privacy techniques used in a study area. Chapter five is about conclusion, recommendation and suggestion for further research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Definition of terms

Privacy: An individual’s desire to limit the disclosure of personal health information and avoidance of notice or display the patients should have control over how their medical records used through provision of consent (Tertulino, Antunes & Morais, 2024).

Electronic Medical Record: The term Electronic Medical Record is a digital version used to define an electronic record system used by the general practitioners to record patient clinical information like identification, prescription, laboratory test results etc (Uslu &Stausberg, 2021).

E-Health: “The cost-effective and secure use of information and communications technologies (ICT) in support of health and health-related fields, including health-care services, health surveillance, health literature, health education, knowledge and research” (Tanwar, Tyagi & Kumar, 2019).

EHR “An Electronic Health Record (EHR) is defined as a collection of various medical records that get generated during any clinical encounter or events” (Vikaspedia, 2019)

Health Information Technology: “The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, health data, and knowledge for communication and decision making” (Herasevich, & Pickering, 2021).

Health Informatics: "Interdisciplinary study of the design, development, adoption, and application of IT-based innovations in healthcare services delivery, management, and planning." (Lynda & Hardy, 2024).

Information Security: Measures used to protect the confidentiality, integrity and availability of data and information system (Roohparvar, 2020).

2.2 Privacy on Previous Studies

Privacy are factors that play significant role in the acceptance of any healthcare technology (Kim, 2024). Despite the fact that EMRs have many advantages, the present technologies are insufficiently utilized to understand its maximum capacity while keeping up patients' information privacy.

Healthcare adopters and doctors are still in great worry about the privacy and security issues of the patients' data being untreated. Moreover, privacy and security issues remain a major barrier to adoption of EMR (Tawalbeh, Muheidat, Tawalbeh & Quwaider, 2020). (Alhur, 2024) believes that understanding these barriers and having the right strategy to deal with these issues will ensure the success of EMR implementation.

The most common problems encountered by the user of EMR are security, privacy, and confidentiality (George & Bhila, 2019). There is lot of challenges in EMR implementation such as legal issues, including privacy and security aspects where there are insufficient security standards for EMRs users. This is why is considered as a critical issue for doctors and patients.

(AlQudah, Al-Emran, & Shaalan, 2021) describe EMR systems in general; theories related to technology adoption, issues related to the adoption of EMR and address issues related to certification, security, privacy, and confidentiality. (Lakbala & Dindarloo, 2014) Describe the physician’s attitude and perceptions of important EMRs functions, anticipated utilization of EMR functions and issues affecting the EMRs.

Moreover, without privacy assurances, patients may face problems of whether they should disclose information to health care providers to enhance health care or withhold information to avoid inappropriate use (Nijor, Rallis, Lad & Gokcen, 2022).

2.3 Empirical Review

2.3.1 EMRs Privacy in the World

The United States Health Insurance Portability and Accountancy Act (HIPAA), enacted in 1996, have been instrumental in establishing safety criteria around such elements in the health domain (USA, 1996).

The research done by (Tanwar, Tyagi& Kumar, 2020) from Taiwan about the Security and privacy of personal health record, electronic medical record and health information show that, the analysis was done from 13,960 citations of 410 articles and the results shows that, the designer of electronic health information system must avoid unauthorized use and hacker attacks.

Wrongful disclosure of individually identifiable health information is an offense punishable by both financial penalties and jail terms. In the United States, an earlier

2006 survey revealed that 62% of the public held the view that ‘the use of electronic medical records makes it more difficult to ensure patient’s privacy’ (United States, 2006).

2.3.2 EMRs Privacy in Developing Countries

Digital technologies have penetrated every nook and corner of the world. Privacy, confidentiality and security safeguards must embed in all phases of health ICT systems development (Spigel, Samuel, & Christina, 2018).

Systematic research done by (Odai, et al., 2018) in Malaysia based on the effects of privacy and security on the acceptance and usage of EMR shows that most physicians, nurses, pharmacists, and laboratory staff believe that patient records are not well-addressed by the systems in terms of security and privacy. However, the Indian committee in observed that EMR could provide real-time data access and can be used for evaluation in medical care if developed longitudinally (Balsari, et al., 2018).

The study done by (Ginavannee & Prasanna, 2024) on the effectiveness of privacy and security controls on EHR. The research explains the things, which must put in place to secure patients’ information. The research found that, the security rule must contain administrative, technical and physical security. The research analyzes different threats, which can harm the EHR system without shows the privacy mechanism used on that system.

2.3.3 EMRs Privacy in Tanzania

The Personal Data Protection Act No. 11 of 2022 (the Act) was passed on 1 November 2022 as a recognition to the right to privacy and personal security enshrined under Article 16 of the Constitution of the United Republic of Tanzania, 1977. The Act sets minimum requirements for the collection and processing of personal data in Tanzania. The Act applies to both public and private institutions with the responsibility to collect and process personal data in Tanzania. The Act was prepared in order to ensure that the collection and processing of personal data is strictly controlled.

Study done by (Mohamed, 2020) from Mzumbe University on examination of the law and practice about patient's data privacy and confidentiality. The research was investigating how the presence of the law governs patient data privacy and confidentiality and how the country can improve data privacy laws in Tanzania. However, the study does not explain the current state and the mechanisms used to ensure privacy, security and confidentiality implemented in EMR in order to give trust to patients.

2.3.4 Privacy on Other Institutions

Privacy on other institutions like financial institutions implement a comprehensive framework that includes policies, procedures, and controls for protecting customer data. This framework should cover aspects such as data classification, access controls, encryption, data retention, incident response, and disaster recovery. Financial institutions should ensure complete compliance with all data security-related regulations and standards. This includes regulations such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS).

2.4 Block-chain Technology

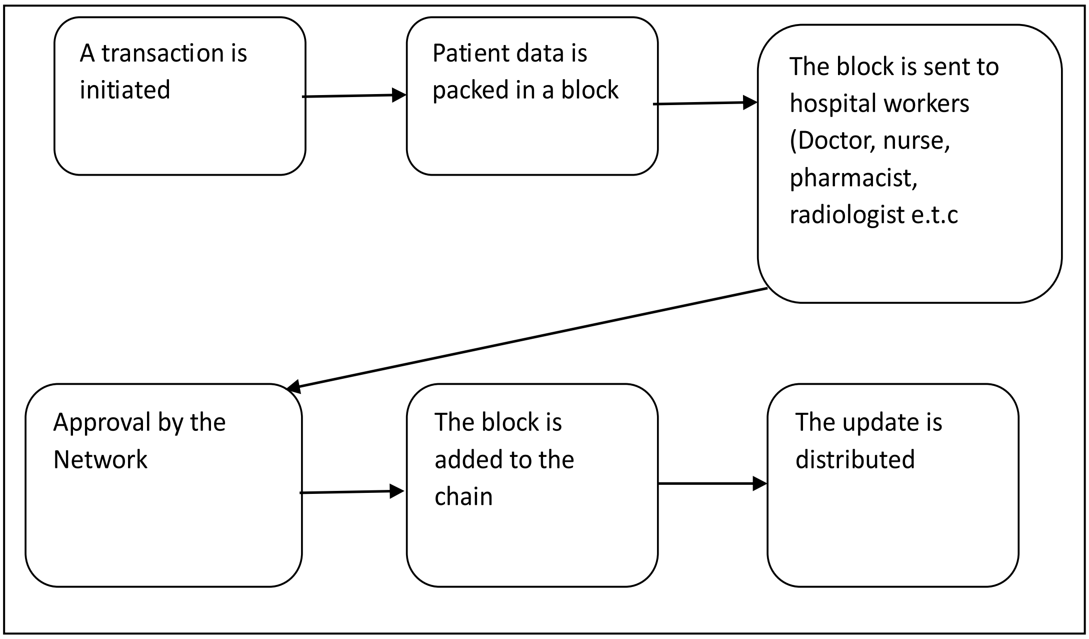
Blockchain is a decentralized, distributed digital ledger technology used to securely record transactions across a network of computers. Each transaction or piece of data is stored in a "block," and these blocks are linked together in a chronological order, forming a "chain." This structure ensures that data cannot be altered or tampered with without altering every subsequent block, which makes blockchain highly secure and transparent (Adusumilli, Damancharla & Metta, 2023). The process about storage, accounting, maintenance, verification and transmission of blockchain data is based on the distributed system structure, using pure mathematical methods rather than central institutions to establish trust relationships among distributed nodes, thus forming a decentralized trusted distributed system.

Fundamentally, it is a set of nodes named verifiers or miners that are responsible for maintaining a trusted record for all transactions via a consensus algorithm in a trust-free environment. As the name implies, a blockchain is made up of many blocks, among which the block refers to the collection of all information communication data in the system within a period of time.

A block is the basic unit that forms blockchain, and each block has a timestamp as its unique mark to ensure the traceability of the blockchain. Using blockchain technology, which is well-known for its successful application in Bitcoin, to secure healthcare data management, has recently piqued public interest.

An open-ended and distributed online database can be created using blockchain technology, which uses data blocks, such as lists of data structures that are linked to one another so that each block refers to the one before it. Infrastructure nodes spread such collaborations rather than keeping them in a centralized storage facility (Gordon & Catalini, 2018). Patients' healthcare data and healthcare provider details from our perspective are included in every block, as well as the timestamp of block generation and the hash of the previous block.

Figure 2.1: How a Blockchain Technology Works.


A transaction is initiated
Patient data is packed in a block
The block is sent to hospital workers (Doctor, nurse, pharmacist, radiologist e.t.c
Approval by the Network
The block is added to the chain
The update is distributed

Source: Compiled from Field Survey (2023)

2.5 Research Gap

Despite the growing adoption of Electronic Medical Records (EMRs) in hospitals, significant gaps remain in understanding the perceived privacy concerns among patients and healthcare providers. Existing studies primarily focus on the technical security aspects of EMR systems, such as encryption and access control, but fail to address user perceptions, trust, and concerns regarding data privacy.

Furthermore, research in Tanzania, lacks a comprehensive evaluation of the effectiveness of privacy-preserving frameworks and the extent to which current EMR systems safeguard sensitive patient information. Additionally, there is limited empirical data on the impact of privacy concerns on patient disclosure behaviors, which may affect the quality of healthcare services. This research seeks to bridge these gaps by analyzing perceived privacy issues in EMRs and proposing a framework to enhance data privacy in government hospitals.

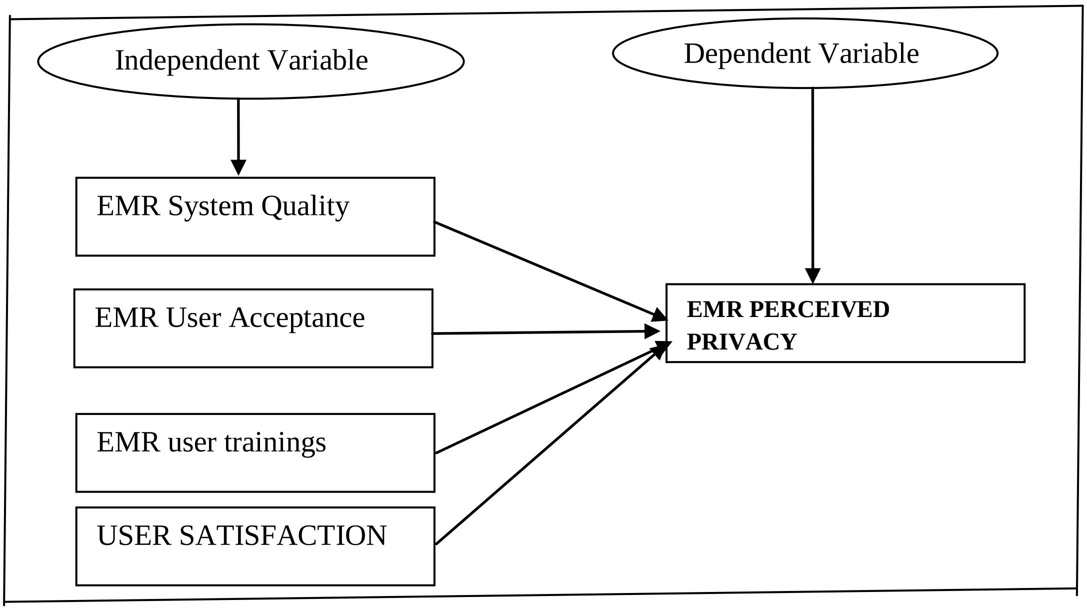
There are many privacy and security breaches done by the use of ICT due to the lack of processes or frameworks to protect it (Akangbe & Charles-Chinkata 2024). Different research done on the issue of privacy of patient’s electronic medical records and shows the advantage and significance of having EMRs (Senishaw, Tilahun, Nigatu, Mengiste & Standal, 2023).

The research done by (Mohamed,2020) in Tanzania proposed to have an assurance of the patient’s data privacy without explaining the current state of privacy, which processes or frameworks implemented to date to ensure patients' data privacy. Therefore, the existing framework does not show how the privacy of the patient’s medical information will be maintained and how the patient is involved in maintaining the privacy of his/her medical information in Tanzania Government hospitals.

2.6 Conceptual Framework

This is a structured approach used to define key concepts, theories, and relationships in a study. It serves as a guide for research by providing a logical structure that connects ideas and helps in understanding how different variables interact. This shows the relationship and connection between independent and dependent variables in the study.

Figure 2.2: Relationship Between Independent and Dependent Variables



Source: Compiled from Field Survey (2023)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research design, approach, and methods that were adopted in the process of data collection and analysis, generally, it will cover the aspects of research design, selection of the study area, study population, sampling procedures, sample size, data collection methods, research instruments, data quality control, data presentation, and analysis.

3.2 Research Design

Research design was referred to the overall strategy that one was chooses to integrate the different components of the study coherently and logically; thereby ensuring the research problem was effectively addressed. This study used mixed method research design. The use of both qualitative and quantitative design constitutes as the blueprint for the collection, measurement, and analysis of data.

3.3 Study Area

This research was conducted in Dodoma-Tanzania. Dodoma is centrally located in Tanzania, which makes it accessible from various parts of the country. This central position allows it to serve as a hub for transportation, trade, and communication. Not only that, but also as the capital city, Dodoma hosts government institutions, ministries, and the official seat of the President. This makes it a focal point for political activities and administrative functions in Tanzania. Due to accessibility of the region, this make the large population to have access to hospital services especially Government hospitals. That why the researcher decides to analyse the perceived privacy of Electronic Medical Records in Government hospitals in Tanzania**.** The research was conducted in Dodoma city municipality based on Dodoma Regional Referral Hospital.

3.4 Study Population

Population is a group of individuals, objects, or items from which samples were taken for measurement. Dodoma Region was easily accessible all year round due to its good road infrastructure relative to the rest of the country. All government offices shifted to Dodoma region which was increased the need for health services due to the large populations that came for access to government services in different offices.

The population of this research was drawn from the selected healthcare workers in Dodoma city municipality. The units of analysis were hospital nurse's staff, doctor's staff, ICT staff and patients. Disregarding the gender variation all staffs and patients were involved in the study, as they expected to provide relevant information about the perceived privacy of Electronic Medical Records in Government hospitals in Tanzania.

3.5 Sample Size and Sampling Techniques

3.5.1 Sample Size

Judgments were made, based on the expected heterogeneity of areas, population groups, locations, and individuals. If heterogeneity is high and units are very different from each other, a large sample was needed, but the sample size also depends on the time and resources available. If heterogeneity was low and units were similar to each other, a smaller sample would suffice.

The researcher was used the Slovin's formular to calculate the sample size of the population by which the known population was 442.

Slovin's formular **n=N/(1+Ne**2)

Where n=sample size

N=Population size

E=margin error

By using the confidence interval of 95% the margin error will be 5%

Therefore, sample size (n)=442/ (1+(442*0.052)

n=210

Therefore, in this study, a sample size of 210 respondents was included in the research for data collection from Dodoma Regional Referral Hospital available in Dodoma City municipality.

By using the "rule of thumb" or judgmental method, the research was decided 108 staffs and 102 patients to participate on data collection.

3.5.2 Sampling Techniques

The purposive sampling technique was used based on the researcher's judgment and the purpose of the study. Two hundred and ten (210) respondents were selected using a purposeful sampling technique including hospital staffs and patients.

3.6 Data Collection Methods

According to the choice of research methods was depending on the research purpose and the research questions asked. This research used multiple methods in data collection.

3.7 Research Instruments

3.7.1 Interview Guide

Interviews were useful in getting the story about a participant's experience. The interviewer was to pursue in-depth information about the topic. Personal interviews were applied to supplement questionnaires; they were conducted purposely for the selected respondents. The interview guide sample was attached as appendix in reference.

3.7.2 Questionnaire

The questionnaire was the main data instrument in this research. The questionnaire was used to collect data on the current state of privacy of Electronic Medical Records in Government hospitals in Tanzania to satisfy patients. The questionnaire was divided into five sections: demographics (3 questions), information privacy concerning electronic medical records (5 questions), information privacy technologies for electronic medical records (3 questions), and EMRs privacy management (4 questions). The questionnaire guide sample was attached as appendix in reference.

3.8 Data Analysis

Various methods were used to organize and summarize data collected, present and evaluate findings, and come up with conclusions. The data was processed and analyzed in line with the objectives of the study. The data was organized, described, coded, and analyzed using Expert survey, Statistical Package for Social Science (SPSS) software version 25, and EPI Info Software version 7.1.3.10 and to derive from simple descriptive statistics, such as frequencies, and percentages to draw different tables and charts.

3.9 Ethical Considerations

The researcher was seeking permission from relevant bodies and letters from the authorities like the Ministry of Health; that were appended to the research project before data collection assuring the respondents that, the research was purely for academic purposes. The study ensures that the confidentiality of the respondent’s information was upheld. The research permit letter from ministry of health was attached as appendix in reference as evidence.

CHAPTER FOUR

RESULTS AND DISCUSSION

1.1 Introduction

This chapter presented the results and discussion of the findings. It was intended to answer the problems of the study. In the findings, the researcher described the process of calculating and presenting the results of the data.

The researcher did the research and got the complete data from all the research instruments including questionnaires, interview and focus group discussion. To gain the objectives of the research, the researcher had analyzed the data systematically and accurately as shown below. The data was analyzed in order to draw conclusion about the objectives of the study. The researcher described the findings and discussion in this chapter in the following parts: -

By using the “rule of thumb” or judgmental method due to the reason that the study was using purposive sampling method, the researcher was decided to take 108 hospital workers and 102 patients in order to make a total of 210 respondents for analyzing the perceived privacy of electronic medical records in government hospitals in Tanzania.

4.2 Respondent’s Occupation

The data collected from six different staffs where 36.1% are Nurse, 18.5% are Doctors, 18.5% receptionist, 13% ICT Specialist,7.4% Laboratory technician, 5.6% Pharmacist and 0.9% radiologist as Table 4.1 shows below.

Table 4.1: Respondent’s Occupation

Respondent's Occupation					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Doctor	20	18.5	18.5	18.5
	Nurse	39	36.1	36.1	54.6
	Pharmacist	6	5.6	5.6	60.2
	Laboratory Technician	8	7.4	7.4	67.6
	Radiologist	1	.9	.9	68.5
	ICT Specialist	14	13.0	13.0	81.5
	Receptionist	20	18.5	18.5	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

4.3 EMR Characteristics Use

According to the analysis from Table 4.2, this implies that, most of the staffs have enough knowledge and experience of using the EMR system. The analysis helps to know if the respondent of the particular organization has enough knowledge on using the EMR system. The output shows that 7.4% of the workers have 6 months to 1-year experience of using EMR, 42.6% shows the workers have 1 to 2 years’ experience while 50% shows that they have above 2 years’ experience of using the EMR system.

Table 4.2: For How Long Have you Been Using EMR?

For how long have you been using EMR?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6 months to 1 year	8	7.4	7.4	7.4
	1 to 2 years	46	42.6	42.6	50.0
	Above 2 years	54	50.0	50.0	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

The main device used to access EMR at the hospital are desktop computer, 98.1% of the staffs are using desktop computers to access EMR while 1.9% of the staffs use laptop computers as the results shows in Table 4.3.

Table 4.3: What is the Main Device you Use to Access EMR System?

What is the main device you use to access EMR system?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Desktop Computer	106	98.1	98.1	98.1
	Laptop Computer	2	1.9	1.9	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

4.4 Objective One

Determine the EMR privacy techniques used in the study area. Dodoma Regional Referral Hospital (DRRH) were used username and password as a technique to maintain the privacy of the system as 97.2% staffs agreed that they used it as privacy maintenance technique shown in Table 4.4 while Table 4.5 shows 87%, they were used biometrics verification like fingerprint and signature verification for identification and authorization in order to maintain the system privacy.

Table 4.4: Do Staff Need a User Name and Password to Access to the EMR?

Do staff need a user identifier and password to access to the EMR?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	105	97.2	97.2	97.2
	No	3	2.8	2.8	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

Table 4.5: Are Biometrics or other Telephone Technologies Being Used for EMR Identification and Authentication?

Are biometrics or other telephone technologies (fingerprint verification, signature verification) being used for EMR identification and authentication?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	94	87.0	87.0	87.0
	No	14	13.0	13.0	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023).

There is access control to all users, not all users can access all records. Each user has access to data which are particular to his/her field, example; pharmacists only access pharmaceutical works and nothing else likewise to accountant with financial works, Doctors with patient name and tests, laboratory technician with lab works and so forth. Each staff account is monitored in all activity he or she perform which was associated in from login step to logout of the system and everything in between as Table 4.6 shows.

Table 4.6: Which Controls are Implemented to Ensure Privacy of Electronic Data when Transferred from One Place to Another?

Which controls are implemented to ensure privacy of electronic data when transferred from one place to another?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Authentication of the identifiers of the sender and receiver before transfer	7	6.5	6.5	6.5
	Password-protected data files without encryption	82	75.9	75.9	82.4
	Encryption of the information during transfer	3	2.8	2.8	85.2
	post-transfer verification of the appropriate and successful transfer	7	6.5	6.5	91.7
	Privileged Mode	9	8.3	8.3	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023).

4.5 Privacy Techniques

The data shows that, the privacy techniques used in the study area in order to maintain the EMR privacy are as follows: -

They use username and password: - Passwords are a weak form of protection for many reasons. One major reason is that passwords depend on the weakest link in the computer and network security chain. There are several ways in which an intruder can attack password-protected systems. The most common form of attack is password guessing. Many people often choose their own name, username, telephone number as their password also they choose the name of family members, friends or special interests. Whereby, it will be easily for an attacker to find this information and breach the privacy of the EMR.

Biometrics verifications: -This used to enhance security, it is convenience and improve user experience. But in the side of data privacy, biometric authentication systems store sensitive information about individuals, such as their fingerprints or facial features. If the information falls into the wrong hands, it can be used for identity theft or other malicious purposes. Also, biometric authentication is false positives, the system may sometimes incorrectly identify individuals, leading to false positives (Proov, 2018). For example, a fingerprint scanner may not recognize a person's fingerprint if it's dirty or smudged., this can lead to frustration and inconvenience for users.

Not only that, but also Biometric authentication systems has high cost, means is expensive to implement and maintain. The hardware and software required for biometric authentication can be costly, and the systems need to be regularly updated and maintained to ensure their effectiveness (Sarier,2022). Therefore, the privacy mechanism used in the study area it does not show promising of maintaining the patient data privacy because it has a lot of weakness which can breach the data privacy of an EMR.

4.6. Objective Two:

Assessing the state of privacy of the EMR system in the study area.

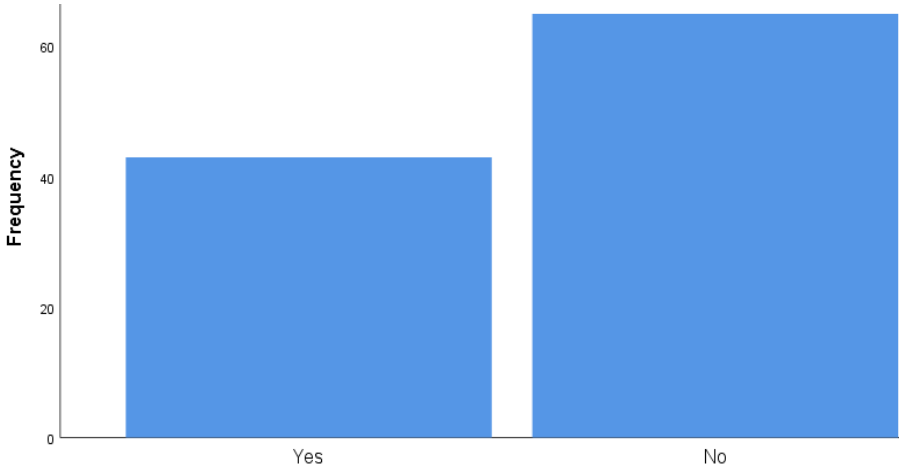
As the results show in Table 4.7, 83.3% of respondents agreed that, the privacy risk assessment is conducted at their working place while Figure 4.1 shows 65% of the staff conclude that, the data confidentiality and privacy policy are not accessible to all staffs. Results from Table 4.8 show that 72.2% agreed that there are no clearly defined roles and access levels for all persons with authorized access to patient EMR.

Table 4.7: Is privacy Risk Assessment Conducted to Staffs?

Is privacy risk assessment conducted to staffs?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	90	83.3	83.3	83.3
	No	18	16.7	16.7	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

Figure 4.1: Is the Data Confidentiality and Privacy Policy readily Accessible to all Staffs?



Source: Compiled from Field Survey (2023)

Table 4.8: Do you have Clearly Defined Roles and Access Levels for all Staffs with Authorized Access to Patient EMR?

Do you have clearly defined roles and access levels for all staffs with authorized access to patient EMR?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	30	27.8	27.8	27.8
	No	78	72.2	72.2	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

1.6.1 Perceived Privacy of the EMR from the Patient

The data was collected from patients and the aim was to analyze how the patient perceived the privacy of their electronic medical records when they were going to get treatment at Government hospitals.

4.6.1.2 Respondent's Gender

The gender of respondents who was participants on answering the questions was 54.9% male and 45.1% female as the Table 4.9 shows. The analysis shows that the number of males is higher than the number of females by the difference of 9.8%.

Table 4.9: Respondent's Gender

Respondent's Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	56	54.9	54.9	54.9
	Female	46	45.1	45.1	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

4.6.1.3 Age of the respondent's

The analysis from Table 4.10 shows that 21 respondents have the age between 18-25 with 20.6%, 25 respondents have the age between 26-35 with 24.5%, 35 respondents have the age between 36-45 with 34.3% and 21 have the age above 45 years with 20.6%.

Table 4.10: Respondent's Age

Respondent's Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	21	20.6	20.6	20.6
	26-35	25	24.5	24.5	45.1
	36-45	35	34.3	34.3	79.4
	Above 45	21	20.6	20.6	100.0
	Total	102	100.0	100.0	

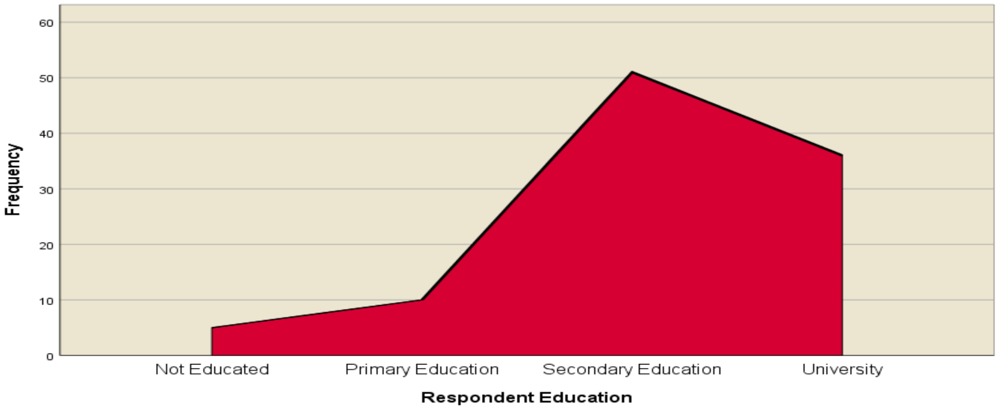
Source: Compiled from Field Survey (2023)

The data shows that the respondents have grown up enough physically and mentally to understand the research questions and answer them correctly.

4.6.1.4 Education Level of the Respondent

Figure 4.2 shows the education level of the respondents. The total number of people who responded is 102 of which 4.9% not have formal education, 9.8% have primary education, 50% have secondary education and 35.3% have University education. Therefore, the results show that 85.3% of the respondents have a secondary level of education and above. This implies that the respondents understanding capacity towards the research questions is high and the answers they provide are reasonable and valid.

Figure 4.2: Respondent's Education



Source: Compiled from Field Survey (2023)

Due to the education level of the respondent's, 85.3% have enough capacity to understand the questions clearly. This makes the data collected from the respondents to be Valid.

4.6.1.5 Access Service from Government Hospitals

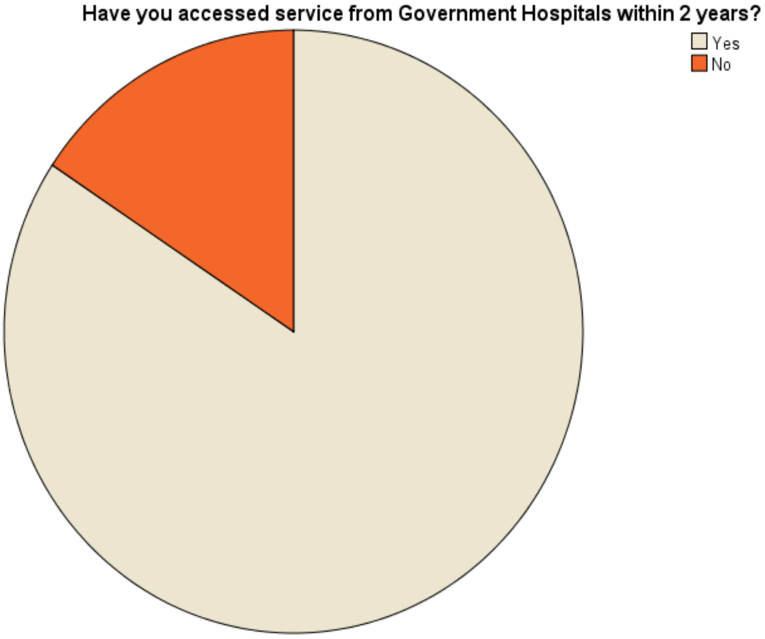
Table 4.11 and Figure 4.3 show that 84.3% of the respondents have access to Government hospitals within 2 years. This implies that the respondents who interviewed have experience of getting service by using EMR systems from Government hospitals.

Table 4.11: Access Service from Government Hospitals

Have you accessed service from Government Hospitals within 2 years?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	86	84.3	84.3	84.3
	No	16	15.7	15.7	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

Figure 4.3: Access service from Government Hospitals



Source: Compiled from Field Survey (2023)

4.6.1.6 Perceived Privacy of EMR from Patient

As the results show in Table 4.12, 64.7% of respondents conclude that they have worries about the privacy of their electronic medical records because 75.5% of them do have not enough knowledge about how the privacy of their medical records is managed electronically as Table 4.13 shows.

Table 4.12: Worries About the Privacy of Your EMR

Do you have any worries about the privacy of electronic medical records?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	36	35.3	35.3	35.3
	Yes	66	64.7	64.7	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

Table 4.13: Do you have Knowledge how the Privacy of your EMR is Managed?

Do you have enough knowledge how the privacy your EMR are managed?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	25	24.5	24.5	24.5
	No	77	75.5	75.5	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

4.6.1.7 Experience with EMR when Getting Health Services?

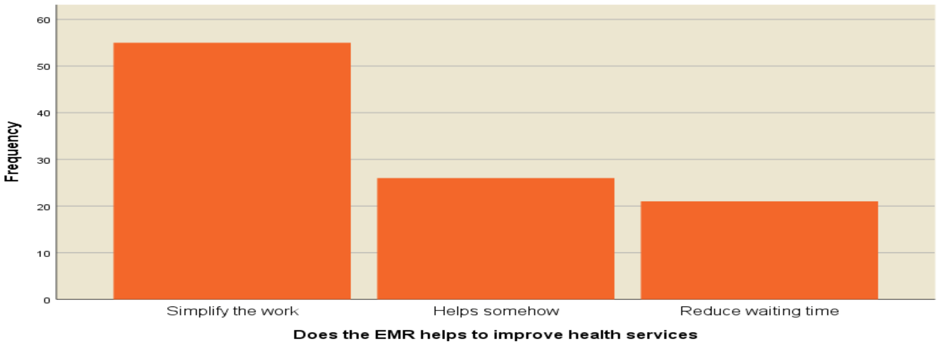
According to the respondent's experience on using EMR at Government hospitals, 85.3% conclude that EMR is best than the paper records as 53.9% says it simplify works, 20.6% says it helps to reduce waiting time while 25.5% conclude that it helps to improve the health services as Table 4.14 and Figure 4.4 shows.

Table 4.14: Is EMR best than Paper Records?

Do you think EMR is best than paper records?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	87	85.3	85.3	85.3
	No	5	4.9	4.9	90.2
	I am not sure	10	9.8	9.8	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

Figure 4.4: Does EMR helps to Improve Health Services?



Source: Compiled from Field Survey (2023)

As a result, shows in Table 4.15, 44.1% of the respondents has very bad experience on using EMR when getting health services at Government hospitals due to network problem, 41.2% has good experience on maintaining the patients records while 14.7% has bad experience since their health information's are accessed with many people, they believe that their health issues must be known only with a doctor and no other hospital staffs.

Table 4.15: The Experience of EMR System when you Get a Service

Can you explain the experience of EMR when you get a service?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Good experience on maintaining patient data	42	41.2	41.2	41.2
	Bad experience since Information is accessed with many people	15	14.7	14.7	55.9
	Very Bad experience due to network problem	45	44.1	44.1	100.0
	Total	102	100.0	100.0	

Source: Compiled from Field Survey (2023)

The data shows that, privacy risk assessment is conducted in the hospital but the data confidentiality policy and privacy policy are not accessible to all staff's members who use the EMR system. There is no clearly defined roles and access levels for staffs with authorized access to patient EMR. This implies that, the privacy of the patients EMR are not maintained properly.

The data collected shows that, the patients who participate in the research have more than two years' experience of accessing the hospital service via EMR system. The patients conclude that, they have worries about the privacy of their electronic medical records due to the fact that, they have no enough knowledge or awareness about how the privacy of their medical records are managed electronically.

The patients agreed and conclude that EMR is best than the paper records as other researchers agreed on it. But the patients have very bad experience on using the EMR system when getting health services at Government hospitals due to the network problem. This is the area the Government and healthcare shareholders must watch with close eyes, how to invest the modern network infrastructures in order to improve the services to their customers.

4.7 Objective Three

Designing an EMR privacy framework for Government hospitals.

After the researcher determine the EMR privacy techniques used on patient data privacy and assessing the shortcomings of the system on privacy issues. The researcher decided to design the framework which will solve the privacy issues in EMR system. As Table 4.16 show 74.1% of the hospital workers disagreed that they have another way of protecting patient's data privacy. They do not use a built-in encryption to protect the patient's data privacy when used to connect to other networks while 25.9% agree that, they use encryption method when connected with another network. This implies that, there is no enough controls on patients' data privacy.

Table 4.16: The use of Encryption Methods

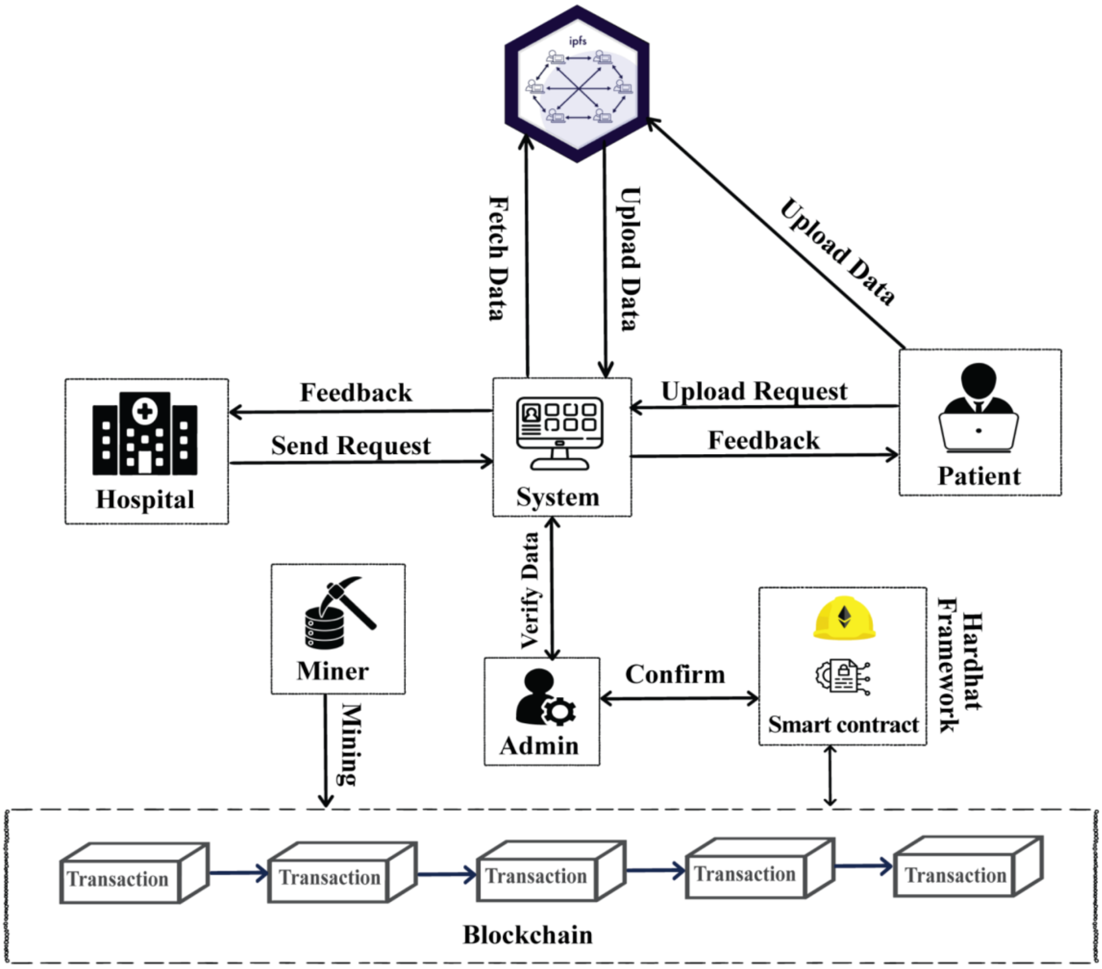
Is there built-in encryption on the methods used to connect to other networks?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	80	74.1	74.1	74.1
	Yes	28	25.9	25.9	100.0
	Total	108	100.0	100.0	

Source: Compiled from Field Survey (2023)

The EMR privacy framework was designed by considering the research objectives, literature reviews, and the results of analyzed collected data from the study. The access control blockchain-based framework provides an exhaustive array of tactics for tackling privacy issues and guaranteeing the privacy of patient information. The blockchain technology strategies encompass robust encryption techniques, access controls, user authentication mechanisms, and privacy assessments.

4.7.1 A Designed Framework

Figure 4.5: A Designed Block-Chain Technology of an EMR Privacy Framework for Government Hospitals.



Source: Designed Framework from Field Survey (2023)

Admin: is responsible for managing, verifying, and controlling access to medical records while ensuring system security and compliance.

The System: is an act as the central hub that connects all stakeholders, processes requests, and ensures secure interactions between patients, hospitals, administrators, NHIF and blockchain components.

Blockchain: The blockchain is an entity that stores the smart contracts, the EMR signature, and encrypted keys.

Patient: The patient, at first, needs to be registered on the hospital's server before meeting with the doctor. After the registration process, the hospital server generates a token for the patient, that serves as a patient's visiting card. A (doctor, nurse, pharmacist, lab technician) generates EMR and the keywords for that patient and further encrypts them both with public key of patient. Encrypted EMR is maintained and stored in hospital system whereas hash value of encrypted EMR is uploaded into private blockchain.

Hospital Stakeholders (doctor, nurse, pharmacist, lab technician, NHIF): The medical service providers generate new block and EMRs for each patient and further broadcast this new block towards a private blockchain of the hospital. The client computers of the hospital have responsibility of verifying the new block. The server of the hospital collects search-able keywords into the private blockchain also creates new block for consortium blockchain. Servers of all remaining hospitals, in consortium blockchain, have responsibility of verifying the new block.

Cloud storage: The cloud stores encrypted EMRs uploaded by the hospital stakeholders.

A smart contract: is a self-executing program stored on a blockchain that automatically enforces and executes the terms of an agreement when predefined conditions are met.

Therefore, by using the firewall method to maintain the patient EMR privacy, the patient privacy may be infringed whenever any third-party individual or organization other than hospital workers attempt to approach patient’s data. In the light of this dilemma, any related research is not done on the same issue. Therefore, the researcher designed a blockchain framework based on EMR scheme of data sharing that uses the PRE (Proxy Re-Encryption) technology for realizing the third-party access towards patient’s data.

4.8 **Objective Four:** Assessing the designed framework for Government hospitals.

By using the rule of thumb for purposive sampling the researcher selects 33 staffs to participate on assessing the designed framework from Figure 4.5. The designed framework was assessed by using focus group discussion and interview. The respondents are 3 Management personnel, 10 Doctors, 10 nurses and 10 ICT experts.

The assessment output are as follows: -

During the focus group discussion and interview as Table 4.17 show 90.9% of the workers agree that firewall has weakness on privacy issues, also the firewalls are beneficial for an average user but in terms of a large organization sometimes it is troublesome. Employees can be restricted from doing certain operations from the policies used by the firewalls. Not only that but also the overall performance of a computer system gets limited with the use of software firewalls.

Table 4.17: Firewall has Weakness on Privacy Issues?

Do you agree that Firewall has weakness on privacy issues?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	30	90.9	90.9	90.9
	No	3	9.1	9.1	100.0
	Total	33	100.0	100.0	

Source: Compiled from Field Survey (2023)

As Table 4.18 and Figure 4.6 show 93.9% of the workers agree that the designed framework if implemented will helps to improve patients EMR data privacy due to its benefits. The designed framework has the following benefits over the firewall: -

1. Trust: Enables trust between participants who don’t know each other.
2. Decentralized structure: Enables real-time data sharing among hospital workers like nurses, doctors e.tc while reducing point of weakness.
3. Improved privacy: Creates an unalterable record of transactions with end-to-end encryption, which reduces fraud and unauthorized activity.
4. Reduced costs: Creates efficiencies by reducing manual tasks such as amending data.
5. Speed: Eliminates intermediaries so transaction can be handled faster than conventional methods.

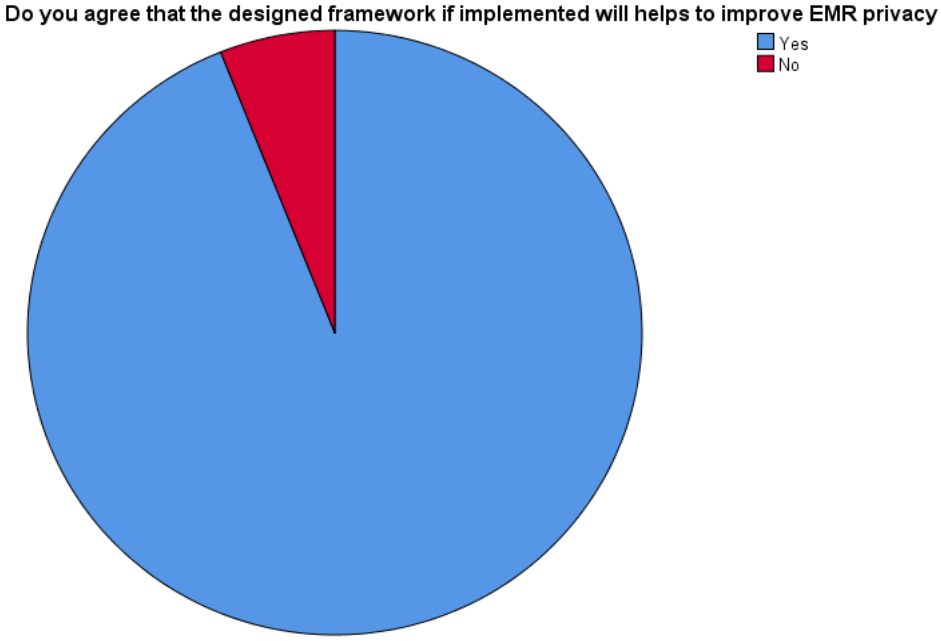
6. Visibility and traceability: Track the origin of a variety of items such as medicine.
7. Immutability: Ensures transactions cannot be edited or deleted.
8. Individual control of data: Gives entities the ability to decide what digital data they want to share, with whom and for how long, with limits enforced by smart contracts.
9. Tokenization: Converts value of an assets into a digital token which recorded and shared via blockchain
10. Innovation: Helps to innovate hospitals and different industries by exploring and implementing blockchain based systems to solve interactable problems.

Table 4.18: If Designed Framework Implemented will helps to Improve EMR Privacy?

Do you Agree that the designed framework if implemented will helps to improve EMR privacy					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	31	93.9	93.9	93.9
	No	2	6.1	6.1	100.0
	Total	33	100.0	100.0	

Source: Compiled from Field Survey (2023)

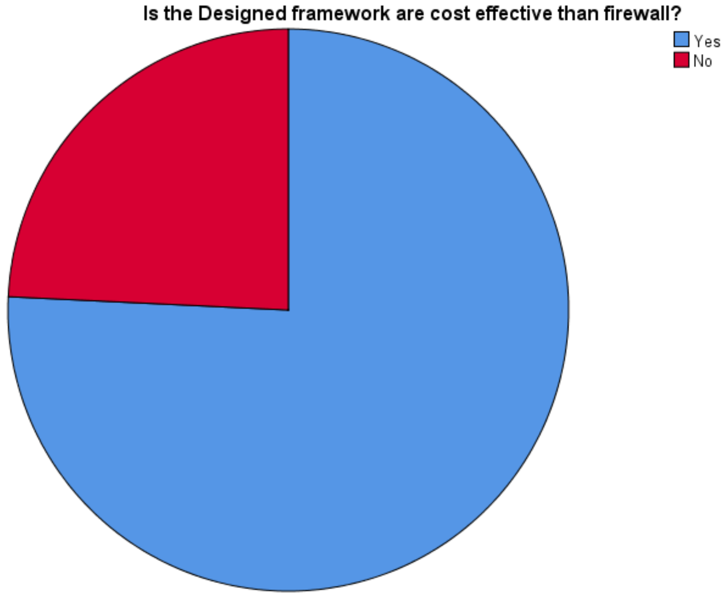
Figure 4.6: If Designed Framework Implemented will helps to Improve EMR Privacy?



Source: Compiled from Field Survey (2023)

As Figure 4.7 show 75.8% of the workers agree that the designed framework will be cost effective if implemented while 24.2% disagree that. The designed framework will Creates efficiencies by reducing manual tasks such as amending data and by easing reporting and auditing.

Figure 4.7: The Designed Framework is cost Effective than the Existing Firewall



Source: Compiled from Field Survey (2023)

Therefore, the benefits of blockchain in healthcare to Government Hospitals can help securely encrypt electronic patient records, protect them from being hacked and preserve the anonymity of individual patients who may be part of the network. This ensures data can be shared seamlessly between healthcare providers and third-part user with minimal privacy concerns.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.0 Introduction

This research aimed at analyzing the perceived privacy of an electronic medical records of Government hospitals in Tanzania a case of Dodoma regional referral hospital. This chapter provides a summary of research findings, conclusion and lastly recommends /suggests some of the measures to be taken on how to maintain the EMR privacy of the patients.

5.1 Conclusion

In this study, the research analyzed several questions regarding the perceived privacy of electronic medical records in government hospitals. The patients experience on perceived privacy on their EMR data shows that, many of the patients have worries about the privacy of their EMR due to the lack of enough knowledge on how the privacy of their health data is managed.

Not only that, but also the privacy techniques and framework used in the study area does not helps to deal with the EMR privacy issues due to the weaknesses it has. Therefore, the researcher introduces a blockchain framework technology which helps to overcome the existing weakness of the ways used to maintain the EMR privacy in the study area.

5.2 Recommendations

Since it has been observed that, patient EMR privacy are very important and is the global concern, the following recommendations are suggested as a solution to improve the perceived privacy of EMR system in government hospitals: -

1. Even though respondents are comfortable with the EMR system, privacy concerns are still there. Because the quality of health care depends on accurate information, patients should be free of any concerns related to their privacy. It is difficult to build public trust after full implementation of the EMR system. Therefore, government and other responsible bodies should implement and enforce strategies to strengthen privacy in this early stage.

2. In this study some EMR users identified that the training they took didn’t prepare them fully to keep patient data privacy. Therefore, these problems must be resolved by MOH, the hospitals or by responsible bodies as quick as possible.

3. In this study patients said they have never told how their health data is being stored and processed. Health care providers should inform their patients in order to avoid confusion and build public trust.

4. All patients and users need to be included before adopting new technologies. Therefore, the ministry of health should communicate the patients to empower consumers to play a greater role in their own care.

5. The study needs to be conducted to further investigate the strength and weakness of the designed framework on solving the EMR privacy challenges and realization of its potential benefits.

REFERENCE

Acheson, E., & Evans, J. (1964). Section of Epidemiology and Preventive Medicine; A Review of the Method with some preliminary results. Royal Society of Medicine, 57, 269.

Adusumilli, Sri Bhargav Krishna, Damancharla, Harini & Metta, Arun. (2023). Enhancing Data Privacy in Healthcare Systems Using Blockchain Technology.

Akangbe, Raphael, Charles-Chinkata & Tyna (2024). Dealing with Data Breaches on Patient's EMR Sensitive Data: A Comprehensive Approach. Frontiers in Digital Health.

AlQudah, A. A., Al-Emran, M., & Shaalan, K. (2021). Technology Acceptance in Healthcare: A Systematic Review. Applied Sciences, 11(22), 10537. https://doi.org/10.3390/app112210537

Charles, S. (2018). EHR vs. EMR: Is there any difference? Technology Advice.

George, J., & Bhila, T. (2019). Security, Confidentiality and Privacy in Health of Healthcare Data. International Journal of Trend in Scientific Research and Development (IJTSRD), 3 (4).

Haux, R. (2022). Health information system – past, present, future, Revisited. International Journal of Medical Informatics, 75 (3-4), 268-281.

Kim, S. D. (2024). Application and Challenges of the Technology Acceptance Model in Elderly Healthcare: Insights from ChatGPT. Technologies, 12(5), 68. https://doi.org/10.3390/technologies12050068

Lopez, O. (2021). Ensuring the Integrity of Electronic Health Records: The Best Practices for E-Records Compliance. Routledge.

Lopez, O. (2022). Data Integrity in Pharmaceutical and Medical Devices Regulation Operations: Best Practices Guide to Electronic Records Compliance. Routledge.

Mohamed, H. (2020). Patient's Data Privacy and Confidentiality in Tanzania: Examination of the Law and Practice. Morogoro: Mzumbe University of Tanzania.

Nijor, S., Rallis, G., Lad, B. & Gokcen, N (2022). Patient Safety Issues from Information Overload in Electronic Medical Records. Journal of Patient Safety 18(6): p e999-e1003, doi: 10.1097/PTS.0000000000001002

Nsaghurwe, A., Dwivedi, V., Ndesanjo, W., Bamsi, H., Busiga, M., Nyella, E., et al. (2021). One country's journey to interoperability: Tanzania's experience developing and implementing a national health information exchange. 21 (1).

Odai, E., Zaidan, A., Alwi, N. H., Zaidan, B. B., Alsalem, M. A., & Albahri, O. S (2018). Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis.

Roohparvar, R. (2020). What is information security? Definition, principles, and policies. Retrieved from https://www.infoguardsecurity.com/what-is-information-security-definition-principles-and-policies.

Sarier, N.D (2022). Privacy Preserving Biometric Authentication on the blockchain for smart healthcare. Pervasive and Mobile Computing, Volume 86, ISSN 1574-1192, https://doi.org/10.1016/j.pmcj.2022.101683.

Senishaw AF, Tilahun BC, Nigatu AM, Mengiste SA, Standal K (2023) Willingness to use electronic medical record (EMR) system and its associated factors among health professionals working in Amhara region Private Hospitals 2021, Ethiopia. PLoS ONE 18(5): e0282044. https://doi.org/10.1371/journal.pone.0282044

Shanholtzer, M. B., & Ensign, A. (2025). Integrated Electronic Health Records (4th ed.). McGraw-Hill Education.

Spigel, L., Samuel, W., & Christina, V. (2018). mHealth Data Security, Privacy, and Confidentiality: Guidelines for Program Implementers and Policymakers.

Sudeep, T. Sudhanshu, T. & Kumar, N. (2020). "Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms, and Solutions.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

Tertulino, R., Antunes, N. & Morais, H(2024). Privacy in electronic health records: a systematic mapping study. J Public Health (Berl.) 32, 435–454. https://doi.org/10.1007/s10389-022-01795-z

United States Code. (2006). Public Law 104-191; THE PUBLIC HEALTH AND WELFARE.

USA. (1996). The Health Insurance Portability and Accountability Act; Security Rule.

Uslu A & Stausberg J. (2021). Value of the Electronic Medical Record for Hospital Care: Update from the Literature, Journal of Medical Internet Research. Vol.23, no. 12, https://doi.org/10.2196/26323.

Vikaspedia. (2019). Electronic Health Record Standards. India: Ministry of Health and Family Welfare.

Vocabulary.com (2025) Dictionary, Vocabulary.com, https://www.vocabulary.com/dictionary/availability. Accessed 17 Mar. 2025.

APPENDICES

Appendix 1: Staffs QUESTIONNAIRE

Questionnaire guideline for Analyzing the perceived privacy of Electronic Medical Record (EMR) System in Government Hospitals Tanzania.

Dear respondents,

I am a student in the faculty of science, Technology and Environmental Studies from Open University of Tanzania. I am pursuing a Master of Science in Information Technology and Management. This questionnaire is designed to be completed by medical practitioners in Government Hospitals. This tool includes questions for **ANALYZE THE PERCEIVED PRIVACY OF ELECTRONIC MEDICAL RECORDS (EMR)** in Government Hospitals Tanzania. Please I need your cooperation, kindly assist to fill the required information below:

SECTION A: Demographic Characteristics

Kindly, select the correct number among the given alternatives: -

1. Occupation

    1. Doctor
    2. Nurse
    3.Pharmacist
    3.Recepitionist
    4. Laboratory technician □
    5.Radiologist
    6. ICT Specialist
    7. Receptionist

2. For how long have you been using EMR?

    1. Less than 6 months
    2. 6 months to 1 Year □
    3. 1 to 2 Years
    4. Above 2 Years

3. What is the main device you use to access EMR system?

    1. Desktop Computer/ Terminal
    2. Tablet PC □

3. Laptop
4. Slate

4.Do staff need a user identifier and password to gain access to the EMR system?

1. Yes

2. No □

3. Not applicable (non-computer situation)

5.How are EMR user identifiers and passwords issued to users? (Please select all that apply.)

1. In person

2. By telephone

3. Through e-mail □

4. Other (please specify):____________

6. Are biometrics or other technologies (e.g. fingerprint verification, signature verification, hardware tokens or smart cards) being used for EMR user identification and authentication?

1. Yes □

2. No

7.Which of the following conditions must be met before releasing patient health data for individual health care? (Please select all that apply.)

1. Verification that patient consent was obtained

2. Confirmation that data have been reviewed for accuracy

3. Removal of direct patient identifiers from released records

4. Documentation of the review of a request to verify that the minimum amount of data needed to satisfy the purpose is being released

5. Acquisition of formal approval for the data release

6. Not specified □

7. Other (please specify):__________________

SECTION B: EMR use Environment

QN8. Based on your experience with EMR, please tick (√) the extent to which you agree (or disagree) with the following statements:

s/no	QUESTION	I DON'T KNOW	STRONGLY DISAGREE	DISAGREE	AGREE	STRONGLY AGREE
1	I received adequate training on how to use this EMR.					
2	My questions about use of this EmR were sufficiently answered.					
3	I receive technical support whenever I need it.					
4	The system downtime is acceptable.					
5	When this EMR system is down, we have policies and procedures to allow the clinic to continue to see patients.					
6	Lab results appear in this EMR in a timely fashion.					

QN9. How often do you use EMR rather than a paper record in the following situations?

s/no	QUESTION	NEVER	OCCASIONALLY	FREQUENTLY	ALWAYS
1	When you need patient test results				
2	When you need contact information for a patient				
3	When you need to document something in the patient medical record				
4	When you want to identify all of your patients with gaps in their care				

SECTION C: Evaluation of the EMR

QN10. Based on your experience with EMR, please tick (√) the extent to which you agree (or disagree) with the following statements:

s/no	QUESTION	STRONGLY DISAGREE	DISAGREE	AGREE	STRONGLY AGREE
1	To me, use of this EMR is easy.				
2	The EMR screens are intuitive.				
3	This EMR provides all functionalities that I expect.				
4	Overall, I am satisfied with my experience with this EMR.				
5	I would recommend this EMR to other similar practices				
6	My colleagues have negative opinions about this EMR				
7	Use of this EMR interferes with my work.				
8	I would be in favor of ceasing use of this EMR in our practice.				
9	Use of this EMR requires me to do more work compared to what I used to do.				

11.Do you have clearly defined roles and access levels for all persons with authorized access to patient electronic data?

1. Yes □

2. No

12. Do you have clearly defined standard procedures or methods that must be followed when accessing patient electronic data?

1. Yes □

2. No

13. Is the Data Confidentiality and Privacy Policy readily accessible to all staff members in this facility who have access to confidential, patient electronic data? (By "readily accessible," mean that staff can easily access the policy online or in hard copy while at work.)

1. Yes

2. No □

14.Is Patient Information Privacy and its Management reviewed at regular intervals?

1. Yes □

2. No

15.How often do independent auditors review privacy practices?

1. Yearly

2. Every 1–2 years

3. Every 2+ years □

4. Not specified

5. Other (please specify):___________

16.Are staff explicitly informed of their individual responsibilities for protecting the systems (paper-based or electronic) that are used to access and utilize patient electronic data?

1. Yes

□

2. No

17.Are privacy risk assessments conducted?

1. Yes □

2. No

18. Are computers permitted to be connected to more than one network?

1. Yes

2. No □

19. Is there built-in encryption on the methods used to connect to other networks?

1. Yes □

2. No

20. Which of the following physical measures are used for protecting patient privacy while collecting information? (Please select all that apply.)

1. Minimize exchange of information verbally

2. Use a partition or curtain in open rooms

3. Use of a separate room with a soundproof barrier

4. Use of window films that provide visual privacy

5. Use of cover sheets on paper documents to provide visual privacy

6. Use of a computer screen guard that provides visual privacy

7. Use of a work space only accessible to authorized staff

8. No measures in place □

9. Other (please specify):____________________

21. What methods or media are used to transfer electronic data within a site? (Please select all that apply.)

1. Intranet, local area network or wide area network

2. E-mail

3. Internet (via web browser)

4. File transfer protocol (FTP)

5. External hard drive

6. Smart card

7. Other (please specify):__________________

22. What controls are implemented to ensure the privacy and security of electronic data when they are being moved within a site? (Please select all that apply.) (Please select all that apply.)

1. Authentication of the identities of the sender and receiver before information transfer

2. Password-protected data files (with or without encryption)

3. Encryption of the information during transfer

4. post-transfer verification of the appropriate and successful transfer of information

5. None of the above

6. Other (please specify):________________________

23. When transferring data within and between sites, which methods are used to authenticate sending and receiving parties? (Please select all that apply.)

1. Sending and receiving parties are not authenticated

2. Two-factor authentication (TFA)

3. Public key infrastructure (PKI)

4. I don’t know

5.Other (please specify):________________________

Appendix 2: Staffs INTERVIEW GUIDE

Interview guideline for Analyzing the perceived privacy of Electronic Medical Record (EMR) System in Government Hospitals Tanzania.

A. Background Information on Interviewee

1. What is your Job Title?
2. What is your education level?
3. Are you using EMR in your daily functions?
4. For how long you are using EMR system?
5. What challenges do you get when using the system?
6. How do you maintain the privacy of the patient information when using the system?

B. General Questions relating to EMR system

1. What are the techniques used to enhance privacy of the patient EMR?
2. What is the state of the privacy of EMR system?
3. What are the effects caused by privacy issues to the users of EMR?
4. Do you conduct privacy Risk Assessment?
5. Do you have clearly defined roles and access levels for all persons with authorized access to patient electronic data?
6. Do you have clearly defined standard procedures or methods that must be followed when accessing patient electronic data?
7. Is the Data Confidentiality and Privacy Policy readily accessible to all staff members in this facility who have access to confidential, patient electronic

data? (By “readily accessible,” mean that staff can easily access the policy online or in hard copy while at work.)

8. Is Patient Information Privacy and its Management reviewed at regular intervals?

Appendix 3: Patient QUESTIONNAIRE

Questionnaire guideline for Analyzing the perceived privacy of Electronic Medical Record (EMR) System in Government Hospitals Tanzania.

Dear respondents,

I am a student in the faculty of science, Technology and Environmental Studies from Open University of Tanzania. I am pursuing a Master of Science in Information Technology and Management. This questionnaire is designed to be completed by patient who get service from Government Hospitals. This tool includes questions for **ANALYZING THE PERCEIVED PRIVACY OF ELECTRONIC MEDICAL RECORDS (EMR)** in Government Hospitals Tanzania. Please I need your cooperation, kindly assist to fill the required information below:

SECTION A: PATIENT'S INFORMATION

1. Patient's Age
   1. 18-25
   2. 26-35 □
   3. 36-45
   4. 46 above

2. Patient's Gender:

   1.Male □

   2.Female

3. Education level:

   1.Primary education

   2. Secondary education

   3. College education □

   4.University education

   5. Professional education

4. Have you get health services in government hospitals within the two years?

   1.Yes □

2.No

5.Do you know how the privacy of your EMR are managed?

1.Yes □

2.No

SECTION B: PATIENTS EMR PRIVACY ISSUES

6.Do you know who are supposed to access your information in the EMR system?

1.Yes □

2.No

7. Is the system helps to improve the health services?

1.Yes □

2.No

8.Can you explain the experience and challenges you face when getting service in the hospital by using EMR system?.

....

....

....

....

SEHEMU C: TRUST ON ELECTRONIC MEDICAL RECORDS

9.Do you think EMR is safe than paper records?

1.Yes

2.No □

3.I don’t know

10. Are you aware of how your health information is transferred from one system to another?

1.Yes

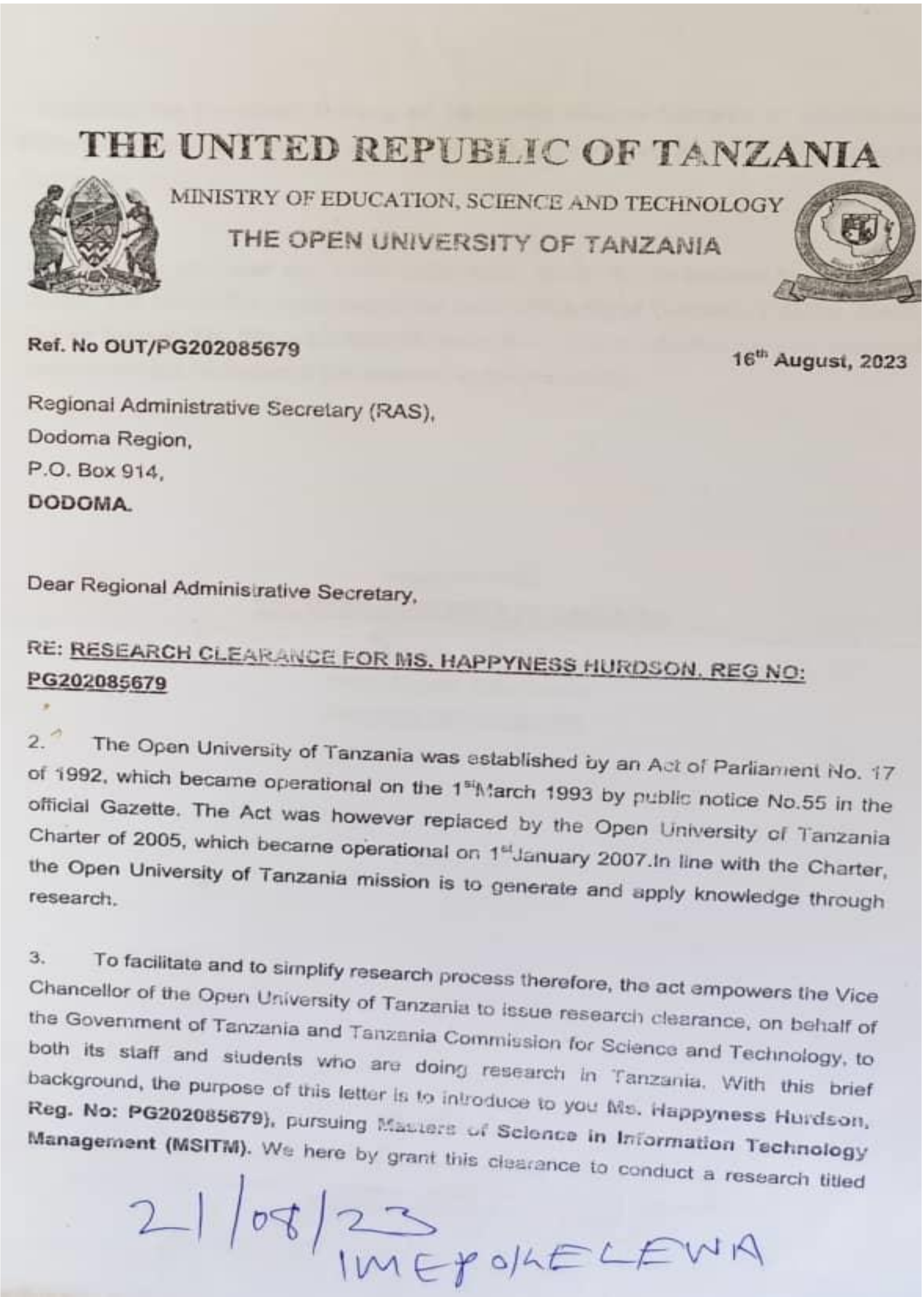
2.No □

11.Do you have any worries about the privacy of your EMR data?

1.Yes □

2.No

Appendix 5: RESEARCH PERMIT



THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

THE OPEN UNIVERSITY OF TANZANIA

Ref. No OUT/PG202085679

16th August, 2023

Regional Administrative Secretary (RAS),
Dodoma Region,
P.O. Box 914,
DODOMA.

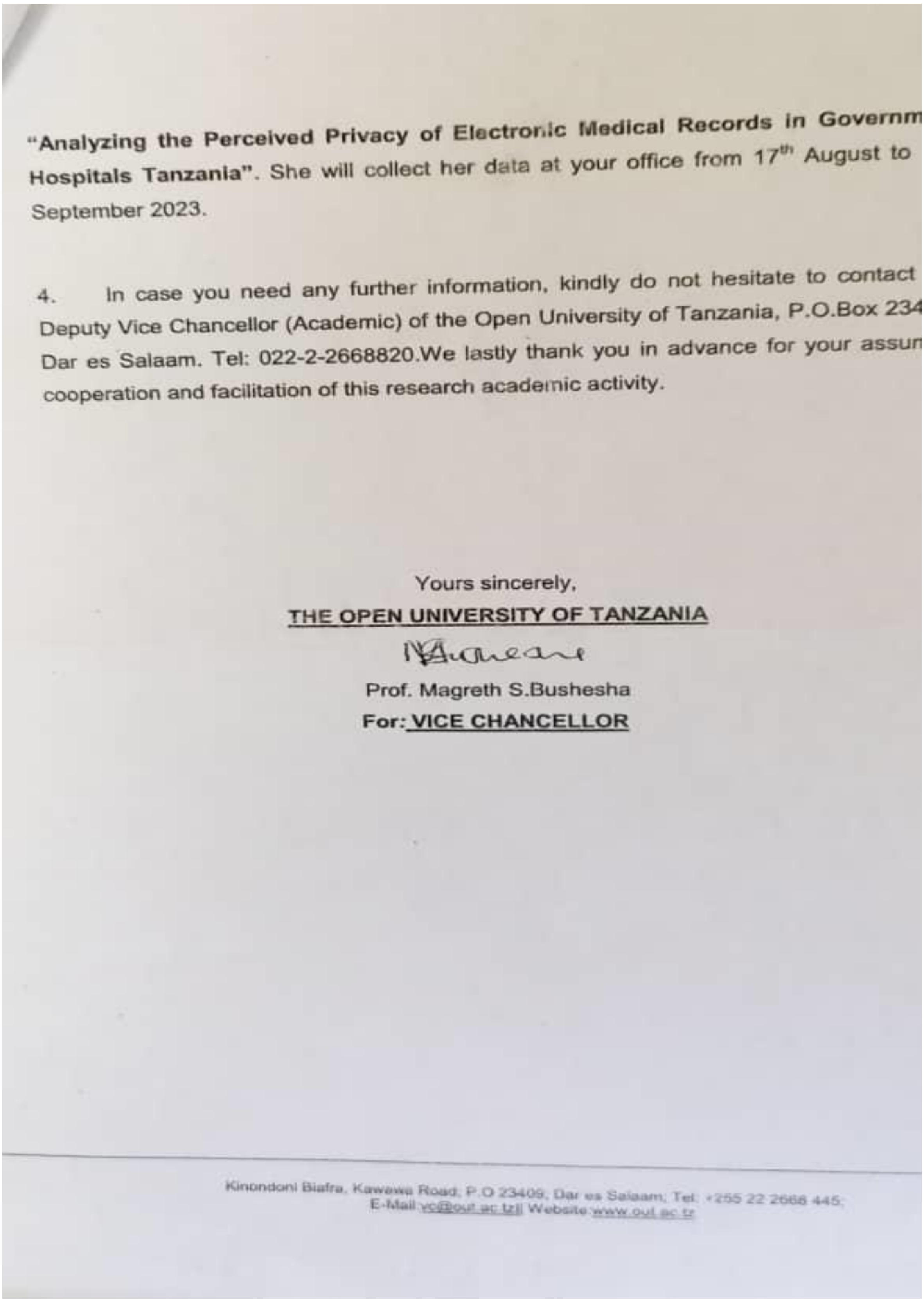
Dear Regional Administrative Secretary,

RE: RESEARCH CLEARANCE FOR MS. HAPPYNESS HURDSON, REG NO: PG202085679

2. The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1st March 1993 by public notice No.55 in the official Gazette. The Act was however replaced by the Open University of Tanzania Charter of 2005, which became operational on 1st January 2007.In line with the Charter, the Open University of Tanzania mission is to generate and apply knowledge through research.

3. To facilitate and to simplify research process therefore, the act empowers the Vice Chancellor of the Open University of Tanzania to issue research clearance, on behalf of the Government of Tanzania and Tanzania Commission for Science and Technology, to both its staff and students who are doing research in Tanzania. With this brief background, the purpose of this letter is to introduce to you Ms. Happyness Hurdson, **Reg. No: PG202085679)**, pursuing **Masters of Science in Information Technology Management (MSITM).** We here by grant this clearance to conduct a research titled

21/08/23
IMEPOKELEWA



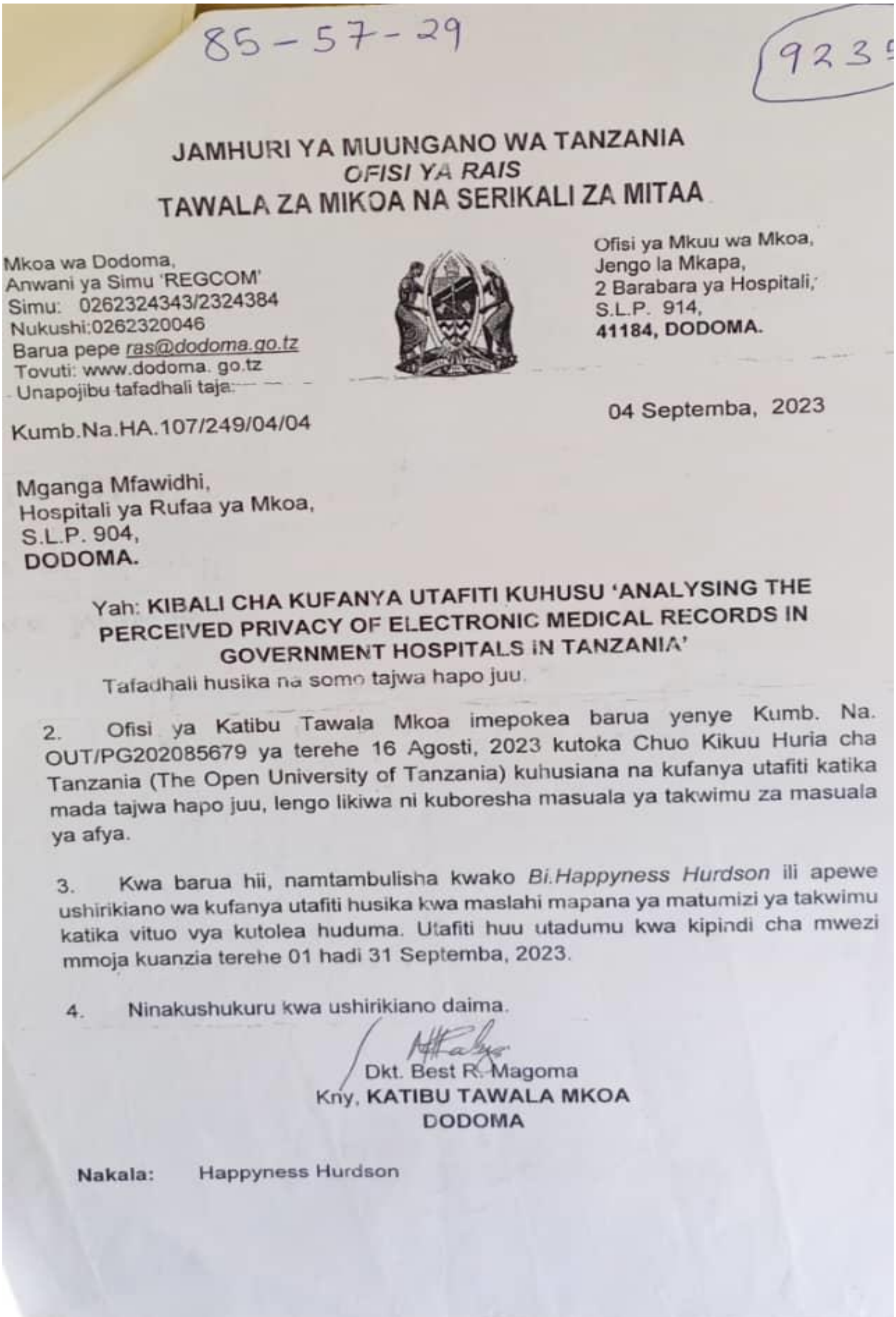
"Analyzing the Perceived Privacy of Electronic Medical Records in Governm Hospitals Tanzania". She will collect her data at your office from 17th August to September 2023.

4. In case you need any further information, kindly do not hesitate to contact Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O.Box 234 Dar es Salaam. Tel: 022-2-2668820.We lastly thank you in advance for your assur cooperation and facilitation of this research academic activity.

Yours sincerely,
THE OPEN UNIVERSITY OF TANZANIA

Prof. Magreth S.Bushesha
For: VICE CHANCELLOR

Kinondoni Biafra, Kawawa Road; P.O 23409, Dar es Salaam; Tel: +255 22 2668 445;
E-Mail:vc@out.ac.tz|| Website:www.out.ac.tz



85-57-29

9235

JAMHURI YA MUUNGANO WA TANZANIA
OFISI YA RAIS
TAWALA ZA MIKOA NA SERIKALI ZA MITAA

Mkoa wa Dodoma,
Anwani ya Simu 'REGCOM'
Simu: 0262324343/2324384
Nukushi:0262320046
Barua pepe ras@dodoma.go.tz
Tovuti: www.dodoma. go.tz
Unapojibu tafadhali taja:

Ofisi ya Mkuu wa Mkoa,
Jengo la Mkapa,
2 Barabara ya Hospitali,
S.L.P. 914,
41184, DODOMA.

Kumb.Na.HA.107/249/04/04

04 Septemba, 2023

Mganga Mfawidhi,
Hospitali ya Rufaa ya Mkoa,
S.L.P. 904,
DODOMA.

Yah: **KIBALI CHA KUFANYA UTAFITI KUHUSU 'ANALYSING THE PERCEIVED PRIVACY OF ELECTRONIC MEDICAL RECORDS IN GOVERNMENT HOSPITALS IN TANZANIA'**

Tafadhali husika na somo tajwa hapo juu.

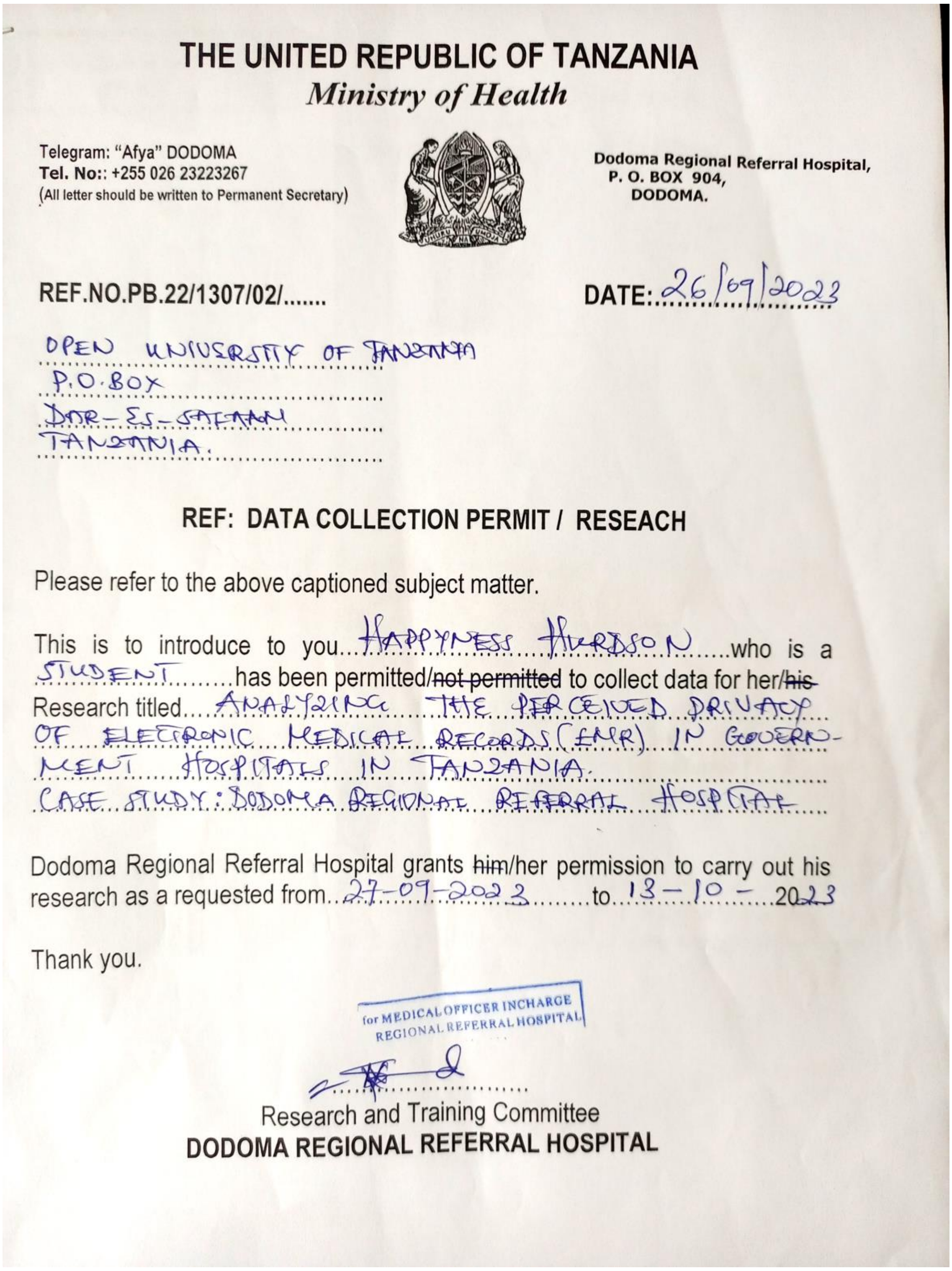
2. Ofisi ya Katibu Tawala Mkoa imepokea barua yenye Kumb. Na. OUT/PG202085679 ya terehe 16 Agosti, 2023 kutoka Chuo Kikuu Huria cha Tanzania (The Open University of Tanzania) kuhusiana na kufanya utafiti katika mada tajwa hapo juu, lengo likiwa ni kuboresha masuala ya takwimu za masuala ya afya.

3. Kwa barua hii, namtambulisha kwako *Bi.Happyness Hurdson* ili apewe ushirikiano wa kufanya utafiti husika kwa maslahi mapana ya matumizi ya takwimu katika vituo vya kutolea huduma. Utafiti huu utadumu kwa kipindi cha mwezi mmoja kuanzia terehe 01 hadi 31 Septemba, 2023.

4. Ninakushukuru kwa ushirikiano daima.

Dkt. Best R. Magoma
Kny, **KATIBU TAWALA MKOA**
DODOMA

Nakala: Happyness Hurdson



THE UNITED REPUBLIC OF TANZANIA
Ministry of Health

Telegram: "Afya" DODOMA
Tel. No:: +255 026 23223267
(All letter should be written to Permanent Secretary)

Dodoma Regional Referral Hospital,
P. O. BOX 904,
DODOMA.

REF.NO.PB.22/1307/02/.......

DATE: 26/09/2023

OPEN UNIVERSITY OF TANZANIA
P.O. BOX
DAR-ES-SALAAM
TANZANIA.

REF: DATA COLLECTION PERMIT / RESEACH

Please refer to the above captioned subject matter.

This is to introduce to you HAPPYNESS HURDSON who is a STUDENT has been permitted/~~not permitted~~ to collect data for her/~~his~~ Research titled ANALYZING THE PERCEIVED PRIVACY OF ELECTRONIC MEDICAL RECORDS (EMR) IN GOVERNMENT HOSPITALS IN TANZANIA. CASE STUDY: DODOMA REGIONAL REFERRAL HOSPITAL

Dodoma Regional Referral Hospital grants ~~him~~/her permission to carry out his research as a requested from 27-09-2023 to 13-10-2023

Thank you.

for MEDICAL OFFICER INCHARGE
REGIONAL REFERRAL HOSPITAL

Research and Training Committee
DODOMA REGIONAL REFERRAL HOSPITAL