

**INFLUENCE OF SECURITY MONITORING PRACTICES ON SECURITY  
OF ELECTRONIC HEALTH RECORDS IN TANZANIAN PUBLIC  
HOSPITALS**

**ERNEST GODSON**

**A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS  
FOR AWARD OF DEGREE OF DOCTOR OF PHILOSOPHY IN  
MONITORING AND EVALUATION OF THE OPEN UNIVERSITY OF  
TANZANIA**

**2023**

**CERTIFICATION**

We the undersigned, certify that we have read and now recommend for acceptance by the Open University of Tanzania the thesis titled: **Influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals:** in fulfilment of the requirements for the degree of Doctor of Philosophy of the Open University of Tanzania.

Prof. Deus Ngaruko

(Supervisor)

.....

Prof. George Oreku

(Supervisor)

.....

Date

## **COPYRIGHT**

No part of the thesis may be reproduced, stored in any retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the author or The Open University of Tanzania in that behalf.

**DECLARATION**

I, **Ernest Godson**, do hereby declare that this thesis is my own original work and has not been presented and will not be presented to any other university for a similar or any other degree award.

.....

Signature

.....

Date:

## **DEDICATION**

This thesis is dedicated to my beloved parents, my wife Helena, lovely daughter Ester and sons Evin and Ezra for their love, prayers and encouragement during the entire study period.

## **ACKNOWLEDGEMENT**

First and foremost, I am most grateful to the ALMIGHTY God for giving me strength, wisdom and healthy during the entire time while doing this study. I say: Thank you Lord.

Furthermore, I would like to express sincere appreciation to my supervisors, Prof. Deus Ngaruko and Prof. George Oreku for their perseverance, unwavering support, untiring mentoring, continuous supervision, advice and insight throughout this study. Without their unwavering encouragement and motivation, this thesis could not have been finished.

I am also thankful to my employer, Dar es Salaam University College of Education for granting me the study leave to accomplish this study. Furthermore, my special appreciation and thanks go to the Medical in charge Officers of the selected public hospitals such as Dodoma Regional Hospital, Iringa Regional Hospital, Mount Meru Regional Hospital, Maweni Regional Hospital, Temeke Regional Hospital and Sekou-Toure Regional Hospital for granting permission to conduct this study in their hospitals and providing me with all the required support. My sincere appreciation also goes to all the staff members of the selected public hospitals who willingly participated in this study to meet the study objectives. Moreover, am also grateful to thank my fellow PhD candidates particularly, Mr Finias Dogeje for the fruitful discussion we had together during our study period.

## ABSTRACT

The study aimed to assess the influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals. The study was carried out in six public hospitals each hospital selected from each country zone. A quantitative research approach and cross-sectional research design were used, whereby integrated system theory and theory of planned behaviour were adopted. Data was collected using questionnaire whereby a sample of 300 respondents were involved. Descriptive and inferential statistics were used in data analysis. The study found that security awareness training yielded a positive and significant influence on the security of EHRs (Beta= 0.455,  $P<0.001$ ), security controls assessment had a positive and significant influence on the security of EHRs (Beta= 0.181,  $P<0.001$ ), security automation yielded a positive and significant influence on the security of EHRs (Beta= 0.384,  $P<0.001$ ), and behavioural monitoring yielded a positive and significant influence on the security of EHRs (Beta= 0.056,  $P<0.001$ ). The study concluded that security monitoring practices positively influence the security of electronic health records in Tanzanian public hospitals. The study recommended that the government should conduct policies review to ensure that the existing eHealth policy incorporate the security monitoring practices. Public hospitals should also strengthen security monitoring practices by conducting regular security awareness training to its staff, conducting regular security control assessment to EHRs systems, improve ICT infrastructure and should invest more on security automation and perform behavioural monitoring to its staff to ensure users compliance with security rules, standards and regulations.

## TABLE OF CONTENTS

<b>CERTIFICATION</b> .....	i
<b>COPYRIGHT</b> .....	ii
<b>DECLARATION</b> .....	iii
<b>DEDICATION</b> .....	iv
<b>ACKNOWLEDGEMENT</b> .....	v
<b>ABSTRACT</b> .....	vi
<b>LIST OF TABLES</b> .....	xiii
<b>ABBREVIATIONS AND ACRONYMS</b> .....	xiv
<b>CHAPTER ONE</b> .....	1
<b>INTRODUCTION</b> .....	1
1.1 Chapter Overview .....	1
1.2 Background to the Study .....	1
1.2 Research Problem Statement.....	7
1.3 Research Objectives .....	8
1.3.1 General Research Objective .....	9
1.3.2 Specific Research Objectives .....	9
1.4 Research Hypothesis .....	9
1.5 Significance of the study .....	10
1.6 Scope of the Study .....	10
1.7 Limitation of the Study.....	11
1.8 Organization of the Study.....	11
<b>CHAPTER TWO</b> .....	15
<b>LITERATURE REVIEW</b> .....	15
2.1 Chapter Overview.....	15



2.2	Conceptual Definitions .....	15
2.2.1	Security Monitoring.....	15
2.2.2	Security Controls .....	16
2.2.3	Electronic Health Records .....	17
2.2.4	Security Awareness Training .....	18
2.2.5	Security Assessment .....	18
2.2.6	Security Automation.....	19
2.2.7	Behavioural Monitoring .....	19
2.3	Theoretical Literature Review .....	19
2.3.1	Integrated Systems Theory .....	20
2.3.2	Theory of Planned Behaviour.....	22
2.4	Empirical Literature Review .....	24
2.4.1	Influence of Security Awareness Training on Security of EHRs.....	25
2.4.2	Influence of Security Assessment on Security of Electronic Health Records.....	28
2.4.3	Influence of Security Automation on Security of EHRs.....	33
2.4.4	Influence of Behavioural Monitoring on Security of EHRs.....	37
2.4.5	The Security Controls of Electronic Health Records .....	41
2.4.5.1	Confidentiality .....	41
2.4.5.2	Integrity .....	43
2.4.5.3	Availability .....	43
2.5	Policy Review.....	45
2.6	Research Gap.....	47
2.6	Conceptual Framework .....	48

<b>CHAPTER THREE</b> .....	51
<b>RESEARCH METHODOLOGY</b> .....	51
3.1 Chapter Overview .....	51
3.2 Research Philosophy .....	51
3.3. Research design .....	52
3.4. Research Approach.....	52
3.5. Study Area .....	53
3.6. Target Population .....	55
3.7. Sampling Design and Techniques .....	56
3.8. Variables Measurement .....	58
3.8.1 The Dependent Variable.....	59
3.8.2 The Independent Variables.....	60
3.9. Data Collection Methods .....	62
3.9.2 Pilot Testing.....	63
3.10. Data Processing Methods .....	64
3.11 Data Analysis Methods.....	66
3.11.1 Sampling Adequacy Test.....	67
3.11.2 Autocorrelation Test.....	67
3.11.3 Multicollinearity Test .....	68
3.11.4 Normality Test.....	69
3.11.5 Factor Analysis .....	69
3.11.6 Correlation Analysis .....	70
3.11.7 Regression Analysis .....	70
3.12. Validity and Reliability .....	73
3.12.1 Validity .....	73
3.12.2 Reliability .....	74

3.13.	Ethical Consideration .....	75
<b>CHAPTER FOUR .....</b>		<b>76</b>
<b>RESEARCH FINDINGS .....</b>		<b>76</b>
4.1	Chapter Overview .....	76
4.2	Respondent's Demographic Description .....	76
4.3	Descriptive Statistics .....	79
4.3.1	Descriptive Statistic for Security Awareness Training .....	80
4.3.2	Descriptive Statistics for Security Controls Assessment.....	81
4.3.3	Descriptive Statistics for Security Automation .....	82
4.3.4	Descriptive Statistics for Behavioral Monitoring.....	83
4.4	Correlations Analysis .....	84
4.5	Multiple Linear Regression Testing .....	85
4.5.1	Influence of Security Awareness Training on Security of EHRs.....	85
4.5.2	Influence of Security Controls Assessment on Security of EHRs .....	87
4.5.3	Influence of Security Automation on Security of EHRs.....	88
4.5.4	Influence of Behavioural Monitoring on Security of EHRs.....	89
4.5.5	The Overall Regression Analysis .....	90
<b>CHAPTER FIVE .....</b>		<b>94</b>
<b>DISCUSSION OF FINDINGS.....</b>		<b>94</b>
5.1	Chapter Overview .....	94
5.2	Demographic Profile of Respondents.....	94
5.3	Influence of Security Awareness Training on Security of EHRs.....	95
5.4	Influence of Security Controls Assessment on Security Controls of EHRs..	97
5.5	Influence of Security Automation on Security of EHRs.....	99
5.6	Influence of Behavioural Monitoring on the Security of EHRs.....	101

<b>CHAPTER SIX</b> .....	107
<b>CONCLUSION AND RECOMMENDATIONS</b> .....	107
6.1 Chapter Overview.....	107
6.2 Conclusions .....	107
6.3 Recommendations .....	109
6.3.2 Theoretical Recommendations .....	111
6.3.3 Policy Recommendation.....	112
6.4 Recommendations for Further Research .....	112
6.5 Implications of the Study.....	113
6.5.1 Implications for Practices .....	114
6.5.2 Theoretical Implications .....	114
<b>REFERENCES</b> .....	116
APPENDIX I: Data Collection Tools.....	145
APPENDIX II: Variable Accuracy Testing .....	150
APPENDIX III: Factor Analysis Results .....	161
APPENDIX IV: Research Clearance Letters - OUT.....	167
APPENDIX V: Data Collection Acceptance Letters .....	173

**LIST OF FIGURES**

Figure 2. 1    Conceptual Framework.....50

## LIST OF TABLES

Table 3.1	Description of Sampling Areas.....	55
Table 3. 2	Sampling frame.....	58
Table 3. 3	Dependent Variable Measurement.....	60
Table 3. 4	Measurement of independent variables.....	62
Table 3. 5	Data Processing Matrix.....	65
Table 3. 6	Summary of Reliability Test.....	75
Table 4.1	Sample Description.....	78
Table 4.2	Key descriptive statistics for security awareness training.....	80
Table 4.3	Key descriptive statistics for Security Controls Assessment.....	81
Table 4.4	Key Descriptive Statistics for Security Automation.....	82
Table 4.5	Key Descriptive Statistics for Behavioural Monitoring.....	83
Table 4.6	Correlation Analysis for Security Monitoring Practices on EHRs.....	85
Table 4.7	Regression results for aggregated SAT indicators.....	86
Table 4. 8	Regression results for aggregated SCA indicators.....	87
Table 4.9	Regression results for aggregated SAUT indicators.....	88
Table 4.10	Regression results for aggregated BM indicators.....	89
Table 4. 11	Model Summary.....	90
Table 4.12	Anova.....	91
Table 4.13	Coefficients of Regression in Overall Mode.....	92

**ABBREVIATIONS AND ACRONYMS**

ANOVA	Analysis of Variance
APA	American Psychological Association
CD	Compatible Discs
COBIT	Control Objectives for Information and Related Technologies
EHR	Electronic Health Record
ESG	Enterprise Strategy Group
FFIEC	Federal Financial Institutions Examination Council
EDR	Endpoint detection and response
HIS	Health information system
HIPPA	Health Insurance Portability and Accountability Act
HIMSS	Health Information management system society
ISMS	Information security management system
ICT	Information communication technology
IDS	Intrusion Detection Systems
ITS& R	Information Technology Security Standards and Regulations
IPS	Intrusion Prevention Systems
IT	Information Technology

ISO	International Organization for Standardization
MOHCDGEC	Ministry of Health, Community Development Gender, Elderly and Children
NIST	National Institute of Standards and Technology
PWC	Price Water house Coopers
OUT	Open University of Tanzania
SPSS	Statistical Package for Social Science
TPB	Theory of planned behaviour
TRA	Theory of reasoned action
UN	United Nation
USB	Universal Serial Bus
VIF	Variance Inflation Factor
WHO	World Health Organisation



## **CHAPTER ONE**

### **INTRODUCTION**

#### **1.1 Chapter Overview**

This chapter provide a comprehensive overview of the entire research study. It draws attention to the development of the research problem being addressed, its value and merits, and the particular areas, span and boundaries of conducting and dealing with the problem. It includes components like study's background, statement of the problem, objectives of study, the research hypothesis, significance of study, its scope, and its organization. The components resulted in a literature review that was guided by a certain methodology, which in turn produced the findings presented in chapter four, discussed in chapter five and summarised, concluded, and implied in chapter six.

#### **1.2 Background to the Study**

The development and proliferation of electronic health records (EHR) in healthcare services delivery have provided healthcare organizations with new tools and methods for capturing, processing, and transferring patient data (Mugo & Nzuki 2014). This has resulted in a growing number of hospitals around the world to move from a largely paper-based record keeping environment to an electronic or paper-light one (Zeng, 2016). Despite, EHRs in healthcare service delivery being in its infancy, some African countries like Uganda, Tanzania, and Ethiopia have successfully integrated EHR systems (Scott & Mars, 2015). For instance, in Tanzania currently, there are over 160 digital health or health-related systems, comprising electronic health record systems, mobile health (M-Health), Telehealth and distance-learning technologies,

Ministry of Health, Community Development Gender, Elderly and Children, (MOHCDGEC, 2019). Furthermore, according to (ICT & Telecom, 2019), Tanzania was able to implement digital health services at 1,303 health facilities by March 2018 via the Digital health investment recommendations Roadmap Programme.

However, such advancement has also opened up the possibility of patient data exposure and unauthorized access to confidential and private data connected to patient medication (Zurita & Nhr 2004; Rothstein & Talbott 2007; Gao, Xiangzhu et al., 2013; Olok et al., 2015; Papoutsi et al., 2015; Ponemon Institute, 2017; Nair et al., 2020). This may impede the overall implementation and use of EHRs. Thus, most researchers have highlighted privacy and security breaches as a critical factors affecting acceptance and implementation of electronic health record systems (Papoutsi et al., 2015; Olok et al., 2015; Nair et al., 2020). Murray (2019) claims that since medical data is worth 10 times more than credit card information, the healthcare industry is one of the most sought-after targets for cybercriminals

The Ponemon Institute (2016), reported that African countries are more affected with large number of security and privacy breaches in electronic health records due to the lack of cyber security knowledge and awareness, lack of strong security legislation, policies, technical and physical cyber security measures (Kritzinge 2013). Studies advocate that the existing approaches for data security regulation in Africa is largely inadequate in tackling data security threats (Belle, et al., 2018; Ademuyiwa & Adeniran 2020). The pace at which African countries are able to introduce and revise data security policies and strategies is much slower that the constantly growing global digital and data trends (Ademuyiwa & Adeniran 2020).

From 314,909 breaches and attacks in January 2019 to 580,147 attacks in January 2020, the Tanzanian computer emergency response team reported a startling increase of 54% in network attacks and security breaches in many sectors of the country, including the health sector (Tanzania Computer Emergency Response Team 2020). Moreover, according to the 2016 Tanzania cyber security report, the country is one of the targets of cyber-terrorists, technology spies, hackers, and digital fraudsters in the world (Cybersecurity report, 2016).

According to Freye et al. (2020) security and privacy breaches in Tanzania healthcare facilities is contributed by lack of comprehensive law to regulate the collection, processing, and sharing of personal data including safeguards against the possible violations. Furthermore, the available draft of personal data protection bill 2014 lack a clear definition of what is consent in as far as processing of electronic health personal data is concerned (Msumi 2018). The country is also faced with a problem of lack of harmonization of eHealth data collection policies at the ministry of Health, the e-Government Agency (eGA) and National Bureau of Statistics (NBS) which has resulted by a poor security monitoring practices (Freye et al., (2020).

Security controls has been frequently regarded to be a technological problem with a technical solution. That is basically untrue since security controls is about managing risks (Whitman & Mattord, 2005) and handling risk is about discovering and measuring threats to information assets (Lampson, 2004). Increasing number of users, systems and applications security become more difficult and consequently rises the threats and vulnerability. This has resulted to security monitoring practices emerged as a promising strategy to revolutionize privacy and data breaches in health

information systems (Schneier 2001; FFIEC 2006; Erturk, 2008). The security monitoring represents the need for routinely assessment of security tools and strategies to ensure that it meet the required standards.

The Information Technology Security Standards and Regulations (ITS&R) asserted that security management cannot be achieved without a proper security monitoring practice (Schneier, 2001). When there is any security failure in the systems the security monitoring practices help to be easily identified. FFIEC (2006) demonstrated that security monitoring plays an important role in identifying security control failures prior to the occurrence of a security incident, identifying the security breach or other security incident early enough to provide an efficient and timely response providing support for post-event forensics operations. Security monitoring is considered to be helpful in reducing employee's poor cybersecurity behaviour and increases employee's compliance with security policies in an organization (Glassman et al., 2015). Security monitoring is direct proportional to the security controls in electronic health records as it provides information about potential and actual breakdowns in in electronic health record systems (Montesino & Fenz 2011).

Many organizations have not achieved a success in the implementation of security monitoring practices due to challenges involved in the implementation process (Glassman et al., 2015). The ESG report 2016 indicated that 26% of respondents in North America showed that security monitoring growth has been more strenuous over the two past years, while 46% revealed that network security monitoring has become somewhat more difficult over the past two years. The 18% of respondents revealed that organizations did not have a large enough security staff for network

security monitoring, 17% agreed that organizations lack tools for security monitoring, 17% stated that organization lack processes and tools to perform continuous monitoring of network analysis, 14% indicated that organizations does not have required knowledge for security monitoring and 13% revealed that organizations do not hold the required tools crucial to analyse network data for security goals.

The lack of enough budget for monitoring and evaluation particularly security monitoring practices was also mentioned as one of the limitation to effective implementation of security monitoring practices in many organizations (Batchellor, 2016). The study argued that many organizations do not set enough budget for security monitoring because security monitoring is not a revenue-generating aspect of IT, thus, it is frequently disregarded during the budgeting process in an organization. Furthermore, organizations in developing countries are faced with lack of enough security staff for network security monitoring and lack the required tools and techniques to perform continuous security monitoring as the digitalization of healthcare services are still in its infancy stage (Morgan, 2019).

The contributions of healthy M&E systems particularly, security monitoring practices in developing countries is still questionable. The World Bank analysis of sector wide approach in 6 developing countries indicated that the contributions of M&E systems in Africa including Tanzania is still low. It was revealed that the healthy M&E systems in healthcare sector lack a common understanding on what should constitutes M&E systems, lack of a framework for guiding ministry department and agencies (MDAs) and districts on how to design and build M&E

systems. Human competence on both supply and demand sides of M&E is generally low, resulting to poor quality and use (G.O.T, 2014).

Despite of the available eHealth implementation strategies such as national eHealth strategy (2013-2018), Health sector strategy plan IV (HSSP IV), Tanzania Digital Health Strategic Plan (2017-2023) and monitoring and evaluation strategic framework (MESF 2020-2025) to monitor and evaluate the implementation process, there is no strategy or policy which had critically considered healthy M&E tool particularly security monitoring practices as an important aspect to success of secured electronic health record systems. All of the strategies reviewed had no detailed information on how electronic health records should be secured with consideration of security monitoring practices despite the fact that patient's data are not effectively secured on electronic health systems.

The security and privacy breaches experienced in Tanzanian public hospitals in recent years urgently call for the need to explore the contributions of healthy monitoring and evaluation particularly, security monitoring practices to security of electronic health records since its contributions is still questionable due to limited evidence. Sajid et al., (2016) stated that a failure in conducting a cyber-security monitoring and evaluation is a critical factor contributing to poor minimization of security gap as organization lack an evidence on the effectiveness of its security controls. There is also lack of evidence on how Ministry of Health and public hospitals management acknowledge the role of security monitoring practices in securing patient's information. The existing eHealth policy lack a detailed emphasis on the security controls of EHRs (Kajirunga & Kalegele, 2015).

There are limited research findings showing the influence of security monitoring practices on security of electronic health records in Tanzania. Many studies in Tanzania context (Busagala 2013; Nehemiah, 2014; Kajiruga, et al., 2015; Kanani, 2016; Freye et al., 2020), focused on adoption and use of EHRs, implementation challenges and impacts of EHRs and ignored the security monitoring aspect. Hence, it was important to conduct this study since empirically little has been articulated in Tanzania public hospitals in relation to security monitoring practices. Thus, the study filled the existing knowledge gap, by assessing the influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals.

## **1.2 Research Problem Statement**

The main problem that prompts this study is that security threats and privacy breaches in electronic health records systems such as the manipulation and stealing of patients' health information, have increased dramatically worldwide (Ponemon Institute 2017). The study by the University of Illinois Chicago (2020) reported that up to the 90% of healthcare organizations in the USA have been victims of at least one data breach in the last two years. Also, in Africa, many healthcare organizations have been experiencing the rise of privacy and security breaches in EHRs (Kamau et al., 2018). In Tanzania, as was reported by Nehemiah (2014), healthcare consumers identified hacking (79.5%), malicious software (69%) and illegal access (70%) as the most prevalent threats to EHR systems.

According to Herath and Rao (2009), although tools and technologies are an integral aspect of an organization's security plans, it is argued that they are insufficient on itself to handle security problems. Erturk (2008) stated that it is impossible without

security monitoring to identify the threats and vulnerabilities that led to security events; thus, it is difficult for security managers, administrators to detect and eliminate such threats and vulnerabilities. Thus, the security and privacy breaches in healthcare facilities is growing as less attention has been paid to the security monitoring practices (COBIT, ISO 27001; Glover 2015; Kvavik et al., 2003).

Many reports and strategies regarding implementation, monitoring and evaluation of health information systems such as eHealth strategy 2012-2018, monitoring and evaluation strategic framework (MESF 2020-2025) lack a detailed section on security monitoring practices, furthermore, many studies on electronic health records systems in Tanzania (Busagala 2013; Nehemiah, 2014; Kajiruga, et al., 2015; Kanani, 2016; Freye et al., 2020), has focused on the challenges on implementation, interoperability issues and impacts of EHRs and insufficient attention has been paid to the M&E particularly security monitoring practices.

Lack of knowledge and evidence on the influence of security monitoring practices to security of electronic health records may cause hospital management and policy makers to concentrate on technological solutions and ignore this important aspect hence, hospitals continue to suffer from privacy and security breaches of patient's information. Thus, this necessitate a need to bridge the knowledge and practice gap by assessing the influence of security monitoring practices on security of EHRs in Tanzania public hospitals.

### **1.3 Research Objectives**

This study was guided by the following objectives:



### **1.3.1 General Research Objective**

The general objective of this study was to assess the influence of security monitoring practices on the security of electronic health records in Tanzanian public hospitals.

### **1.3.2 Specific Research Objectives**

The study was guided by the following specific objectives:

- i) To examine the influence of security awareness training on the security of electronic health records in Tanzanian public hospitals
- ii) To assess the influence of security controls assessment on the security of electronic health records in Tanzanian public hospitals
- iii) To examine the influence of security automation on the security of electronic health records in Tanzanian public hospitals
- iv) To assess the influence of behavioural monitoring on the security of electronic health records in Tanzanian public hospitals

### **1.4 Research Hypothesis**

**The research was guided by the following null hypothesis**

- i) Ho1: Security awareness training has no influence on security of electronic health records in Tanzanian public hospitals
- ii) Ho2: Security controls assessment has no influence on security of electronic health records in Tanzanian public hospitals
- iii) Ho3: Security automation has no influence on security of electronic health records in Tanzanian public hospitals
- iv) Ho4: Behavioural monitoring has no influence on security of electronic health records in Tanzanian public hospitals

### **1.5 Significance of the study**

The findings of this study are important to hospital management, researchers and community at large since it facilitate in understanding how M&E practices particularly security monitoring practices influence security of electronic health records in terms of confidentiality, integrity and availability of patient's information. Thus, it may expand their knowledge, influence practices of security monitoring and hence ensure effective security controls in electronic health records in Tanzanian public hospitals.

Furthermore, this study findings and recommendations may result into the review of the existing national policies particularly eHealth policy to ascertain the influence of the use of M&E systems specifically security monitoring in securing electronic health records, this may lead to national efforts to modify the existing policies and to formulate comprehensive security rules, laws and regulations that properly address the current security controls challenges in EHR systems in Tanzania's healthcare sector.

Additionally, this study's findings may inform healthcare practitioners in public hospitals the influence of monitoring and evaluation particularly security monitoring practices, factors affecting effective implementation of security monitoring practices and thus, help to identify the gap in practices and therefore, provide best practices for the improvement of security controls in electronic health records in hospitals.

### **1.6 Scope of the Study**

This study focuses on the influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals. The study was conducted in

six public hospitals from six country zones which were, Mount Meru Regional hospital Arusha region, Northern zone, Temeke Regional hospital Dar es Salaam region in Eastern zone, Dodoma Regional hospital Dodoma region in Central zone, Iringa regional hospital Iringa in Southern highland zone, Sekou-Toure Regional hospital Mwanza in Lake zone and Maweni- Kigoma Regional hospital in Kigoma region Western Zone.

### **1.7 Limitation of the Study**

The rate of data collection and completion of questionnaires was slow. This resulted into taking more period of time than expected (More than six months). The researcher followed up with respondents' multiple times and was eventually able to collect sufficient numbers of completed surveys to obtain a return rate that made data analysis viable.

### **1.8 Organization of the Study**

The study was made up by six chapters. The chapters include chapter one, two, three, four, five and six as stipulated by the Open University of Tanzania research guideline. The contents of each chapter and relationships are described in this section.

Chapter one covers the background of the study, the chapter describes the study's introduction and background, research problem statement, research objectives and research hypothesis, significance, scope of the study and organization of the study. The components of chapter one led to the review of literature in addressing those components. The contents of chapter one (particularly objectives and hypotheses) directed by the contents of chapter two which were attained by certain methodologies

addressed in chapter three. Through this methodology, the findings in chapter four were obtained and discussed in chapter five. The presentation and discussion of findings led to summary, conclusion and recommendation in chapter six.

Chapter two deals with the literature review, it describes how researcher reviewed and critiqued the theoretical and empirical works related to this study. The review of literature addressed the components drawn from chapter one especially objectives/hypothesis. This chapter addressed the research problem formulated in chapter one particularly by reviewing the theories and empirical studies associated to the given problem. It also described the logical relationships among the variables attained from the stated theories and empirical studies in the conceptual framework. The realistic nature of the relationships was guided and achieved through certain methodologies addressed in chapter three of this study. The methodologies resulted to findings and discussion in chapter four and five which eventually lead to the formulation of summary, conclusion and recommendations addressed in chapter six.

Chapter three concerned with the research methodology employed in the study. It portrays how the research problem hinted in chapter one and two is approached, designed, and how its supportive data were collected and analysed. It specifically dealt with the research design, study areas, population, sample size and sampling techniques, method of data collection, variables and their measurements, reliability and validity issues and data analysis methods. The methods guided and achieved the objectives of the study stipulated in chapter one. Furthermore, the method applied in this chapter resulted to the findings and their discussion presented in chapter four and five respectively. Finally, the findings and their discussion obtained through such

methodology produced summary, conclusion and recommendation as addressed in chapter six.

Chapter four represent the study's findings. The chapter shows how the findings of the analysed quantitative data were presented in the study. The objectives were derived in chapter one and supported by theories, empirical studies and logical relationships presented in chapter two. It was also achieved through methodology presented in chapter three of the study. The interpretation, meanings and details of the obtained findings are discussed in chapter five. Such discussion resulted in the summary, conclusion and recommendations of the study addressed in chapter six.

Chapter five deals with discussion of findings derived from chapter four. It discusses such findings with critical analysis. The discussion provided were about the study objectives hinted in chapter one and chapter two of this study. The findings being discussed in this chapter are obtained as the results of application of methodology hinted in chapter three. The discussed results in chapter five led to the summary, conclusion and recommendations of the study as addressed in chapter six (Figure 1.1).

Chapter six displays the summary, conclusion and recommendations of the study. It distinctively concludes the findings of the study by summarizing the key findings and pertinent conclusion of the study. It also presents the recommendations and implications of the study findings. The summary, conclusion and recommendations addressed in this chapter are originally drawn from the chapter one, two, three, four and five.

The study was finalized with a list of references and appendices. The citations and list of references for the study indicated the literature reviewed following American Psychological Association (APA). The appendices address the research instruments used to collect the data for the study which was a questionnaire guide.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 Chapter Overview**

This chapter exhibits the theoretical and empirical literature reviewed during the study. It addresses the research problem hinted in chapter one specifically by conducting critical review of theories to establish the theoretical link among the independent and dependent variables, hence, creating the framework guiding the study. This chapter also reviews empirical studies related to the study to establish the research gaps. The realistic nature of the relationships was achieved through particular methodologies addressed in chapter three which, produced the results in chapter four and their respective discussion in chapter five. Such results and discussion eventually led to the summary, conclusion and review of the implications of the study in chapter six.

#### **2.2 Conceptual Definitions**

##### **2.2.1 Security Monitoring**

According to the Information Technology Services Security Monitoring Standard (2020), security monitoring is a means of verifying that the security policies and procedures of an organizations are followed and are efficient. Security monitoring comprises of activities like the review of: user accounts logs, application logs, data backup and recovery logs, automated system logs etc.

According to NIST (2011), security monitoring is maintaining constant awareness of information security, vulnerabilities and threats to assist organizational risk management decision. FFIEC (2006), stated that the primary purpose of security

monitoring is to check policy compliance, identify noncompliance with the institution's regulations, and identify intrusion to provide an effective response. Since, security monitoring is often an ongoing operational function, it can provide continuous assurance.

This study considers security monitoring practices as a process to ensure that security controls adopted by organizations remain effective and continue to perform as intended to support security controls of information assets of an organization. Kumar (2012) avows that security monitoring involves the collecting events from numerous security log sources, monitoring and evaluating security events, and establishing a plan for long-term event storage.

### **2.2.2 Security Controls**

According NIST (2013), security controls is a safeguard or countermeasure intended to defend the confidentiality, integrity and availability of an information assets or system to ensure it meets its goals. Security controls involve management, operational and technical activities planned to deter, delay, detect, deny or alleviate malicious attacks and other threats to information systems in an organization.

Security controls as defined by ISO / IEC 27002 (2005) include policies, procedures, guidelines, best practices and organizational structures, and software and hardware functionalities. Security controls are developed, applied, tracked, reviewed and improved when necessary to achieve (1) specified information security objectives and (2) mitigate or reduce information security risks.



This study considers security controls as a plan implemented in an organization to protect all assets that are of value to an organization against an unauthorized effort to unfavourably affect the confidentiality, integrity and availability of information system in a given organisation.

### **2.2.3 Electronic Health Records**

According to Health Information management systems society (HIMSS 2012), Electronic health record (EHR) is a longitudinal electronic record of patient health information created by one or more interactions in any setting of healthcare delivery. This data includes patient demographics, progress notes, difficulties, prescriptions, vital signs, previous medical history, vaccines, laboratory information, and radiological results. The EHR automates and streamlines the clinician's workflow. The EHR can support various care-related activities, comprising evidence-based decisions support, quality management, and result reporting, directly or indirectly via an interface.

ISO/TR (2012) describes electronic health records (EHRs) as: Information pertinent to the well-being, health, and quality of life of an individual in computer-process capable form and represented per harmonised information model Lifecycle electronic record (LERs) of an individual that contain or virtually relate to data in multiple electronic medical records (EMRs) and electronic patient records (EPRs) and are to be shared and, or interoperable throughout health information systems.

This study considers electronic health records (EHR) as electronic records systems that comprise documentation of medical care or health data about an individual in a

certain period. Giere (2004) asserts that electronic health records are a machine-processable information entity consisting of patient records of an individual.

#### **2.2.4 Security Awareness Training**

According to Siponen (2000) security awareness training is the state where users in an organization are trained to be aware of and committed to the security mission of organization.

This study defines security awareness training as a formal process for educating users of information systems about cybersecurity accepted practices to better navigate the many cybersecurity risks and threats they may face in their working places.

#### **2.2.5 Security Assessment**

NIST (2013) defines security assessment as the process of analyzing a system or network to determine how secure it is. A security assessment can be as basic as an audit of the company's IT setup or as complex as a multi-month study that covers every possible risk to the enterprise.

In this study security assessment means the process of examining a system or network to find flaws and vulnerabilities. It's a crucial component of security monitoring practices that can assist organizations in identifying and reducing threats and risk.

### **2.2.6 Security Automation**

Petters (2021) defines security automation as the use of technology to integrate security procedures, applications, and infrastructure while requiring the least amount of human intervention.

According to this study security automation is the process of automatically identifying, detecting, and resolving cyber-threats using programmed solutions created specifically for this purpose, with or without human involvement. Security teams deal with a large number of notifications on a regular basis; security automation plays a key role in streamlining these alerts.

### **2.2.7 Behavioural Monitoring**

According to Baillon et al., (2019) behaviour monitoring, a system or a person analyses patterns such as destinations, frequency/periodicity of recognised risk incidents, and/or volumes exchanged, which determine whether the behaviour exceeds identified baseline.

In this study behavioural monitoring refers to the regular checking and controlling of the users' behaviour over a period of time to quickly detect and correct inappropriate behaviour.

## **2.3 Theoretical Literature Review**

The study was guided by two theories: The Integrated System Theory and the Theory of Planned Behaviour. Despite that there are many theories used in information security management and monitoring such as socio-technical theory, activity theory, protection motivation theory, general deterrence theory, social cognitive theory

(Rogers, 1975; Straub 1990; Straub & Welke, 1998; Rhee, Kim, & Ryu, 2009; Ball, Lilly and Cullen, 2010) the integrated system theory and theory of planned behaviour seem to offer more relevance and strength to this study compared to the rest theories reviewed.

### **2.3.1 Integrated Systems Theory**

The integrated system theory has been used to study information security management and security monitoring practices in organizations. The founder of integrated system theory was (Hong et al., 2003). The theory is founded on five theories: (a) security policy theory, (b) risk management theory, (c) internal control and auditing theory, (d) management system theory, and (e) contingency theory. The theory assumed that effective security management and monitoring involve having security policies, effective risk management, contingency plan, route internal control and auditing and proper security management. According to Hong et al. (2003) security controls combines systems, operations and internal controls to guarantee the integrity, confidentiality and availability of data and processes in an organization.

This theory helped to inform the study the critical components to effective security monitoring practices. The five theories from the integrated system theory such as security policy theory, risk management theory, contingency theory, internal control and auditing theory and management theory was adopted to inform the influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals. The policy theory proclaimed that organization need to have effective security policy and regular policy review, risk management theory depicted important constructs to security controls assessment which was the second objective

of this study. The internal controls and auditing theory stated that organizations should implement internal controls and auditing of controls should follow. Contingency theory emphasised on having alternative control plans for effective security monitoring practices in organizations.

This study depicted some of the critical issues from the integrated systems theory to guide the study, first, healthcare organizations can only secure its information systems by having a combined system, operations and internal controls. Second, healthcare organization should conduct policies assessment and review frequently to reach the need of the organizational security desires as suggested by (Gupta et al., 2001). Third, there should be security standards and security strategies to form information security control systems. Fourth, healthcare organizations should establish an internal controls system and there after internal auditing processes need to be implemented to determine its strength. Lastly, healthcare organization should perform a regular risk and vulnerability assessment to ensure healthcare systems are not exposing themselves to unnecessary risks and vulnerabilities. This theory was adopted to guide the two objectives of this study which is influence of security controls assessment and influence security automation using question constructed on Likert scale to quantify respondents' responses based on devised indicators.

Integrated system theory has strength that, it has integrated different standpoints from security policy, risk management, internal controls and auditing, management systems and contingency which is helpful to inform security system administrators, managers about appropriate decisions to make on effective information security monitoring in an organization, this makes it one of the best theories to describe and

explain the influence of security monitoring practices on security controls in electronic health records.

Despite the applicability of integrated system theory, it has some notable weakness that except the contingency theory, all other theories are process-oriented from the top down but lack appropriate procedures (Kwo-Shing Hong et al., 2003). Furthermore, the theory does not completely elaborate the role of behavioural monitoring on security controls in an organization, therefore, to complement the identified weakness the study adopted the theory of planned behaviour.

### **2.3.2 Theory of Planned Behaviour**

The theory of planned behaviour is an extension of the theory of reasoned action (TRA) introduced by (Fishbein & Ajzen (1975). According to this theory, “planned” behaviour is ascertained by “intention,” and “intention” is influenced by “attitude,” “subjective norms, and perceived behavioural control” (Ajzen, 1975). In other words, “attitude” affects “feelings” about doing the behaviour. The theory further stated that when users believed that it is important to “understand and comply” with a particular behaviour, “feelings about compliance” positively affected their intentions to comply.

Furthermore, the theory proclaims that behaviour is a function of beliefs (or information) related to a specific behaviour. Thus, beliefs are the primary drivers of intent and action (Ajzen, Doll, 1992). The beliefs associated with the specific behaviour also relate to the outcomes that will be achieved by performing that behaviour, and the potential costs associated with performing that behaviour. The intentions that measure the effort people are ready to expend to execute a particular

behaviour are thought to capture the motivators that drive behaviour (Beck, Ajzen, 1991).

This theory is built on four dimensions which is attitude, subjective norm, perceived behavioural control and behavioural intention. Using the introduced theory of planned behaviour dimensions, organization can achieve effective security controls. For instance, an individual with a positive attitude of security controls would also have more intention to adhere to security controls. Subjective norms reflect how an individual perceives other people's perceptions of how they behave when they perform behaviour (Ajzen, 1991). All this influence an intention to comply with security controls in an organization.

This study used the theory of planned behaviour which emphasised on creating positive attitude to users for them to adopt security compliance behaviour, the theory argued that if users think a favourable consequence will occur as an outcome of undertaking favourable behaviour he or she will keep on performing such behaviours (Ajzen, 1991). Users will sense more positive about stimulating and joining in the proper information security activities if taught, highly acknowledged and heavily rewarded (Ajzen, 1991). According to this theory, if users lack knowledge, have little understanding in the information security issues particularly information security policies, rules and standards will not effectively participate in security controls. This study adopted this theory to guide the first objective and fourth objective which is the influence of security awareness training and the influence of behavioural monitoring to security of EHRs respectively.

The theory of planned behaviour has its strength that it has a much broader range of drivers than other motivation theories that focus on just three drivers. It also has a substantial body of empirical evidence supporting it, which reflects its utility, applicability and robustness to rigorous testing.

Despite the applicability of theory of planned behaviour in this study, the theory has the prominent weakness that, it does not address the unconscious reasons that can influence person's decision-making. Instead, it focuses on conscious decision-making processes. Nevertheless, the emphasis on conscious decision-making may not accurately capture the complexity that human behaviour entails. Furthermore, this theory did not provide a broad spectrum of motivations as opposed to other motivation theories (e.g., Self-determination theory). However, this weakness does not detract from the usefulness of the theory as it serves to highlight the influences of security awareness training and behavioural monitoring on the security of EHRs. Therefore, the theory of planned behaviour was employed to see how security monitoring practices influence the security of EHRs in Tanzanian public hospitals.

#### **2.4 Empirical Literature Review**

This section provided an empirical analysis of studies related to this topic. Understanding the correlation between the problem and the existing body of knowledge necessitated an examination of previous literature. Furthermore, the review was conducted to form the need for this type of study and to inform the researcher by examining the procedures employed by previous researchers to discover answers to similar research issues to those addressed in this study.



#### **2.4.1 Influence of Security Awareness Training on Security of EHRs**

The study conducted by (Zamir, 2020), on the influence of security awareness to security controls in healthcare organizations found that security awareness training has a positive influence on security controls as it equips healthcare employees with the knowledge necessary to make prudent decisions and handle patient data with appropriate care. The study concluded that training of staff on security policies, developed guidelines and procedures enabled them to make right decisions regarding security controls. The study finding was supported by (Andriole, 2014) which stated that if employees are well educated on grammatical errors, as phishing emails frequently contain misspellings or grammatical errors or are sent from suspicious-looking addresses that resemble the company being impersonated they can make a right decision of keeping themselves away from it. The study concluded that security awareness training will not only improve security compliance but also will increase participation of users to security monitoring practices.

The study by Ban Issa et al. (2020), on concerns among nurses working in the United Arab Emirates related with the use of electronic health records, including privacy, confidentiality, security and patient safety found that inadequate training and awareness on the part of hospital staff, including nurses, were the primary causes of security breaches involving electronic health records (EHR). They added that if nurses are not adequately trained in security policies and security control measures, their participation must be obviously poor. Despite of their results, the study did not explore in detail some important parts of awareness training. Although the findings do not agree with the study hypothesis this study was conducted in the United Arab

Emirates, hence the results may not necessarily reflect the developing countries context like Tanzania. Thus, this study was necessary in order to reflect developing countries context.

Relatedly, a cross-sectional study by Nisreen (2018) on managing information security issues of electronic medical health records in Amman, revealed that healthcare workers in Amman's public hospitals lacked sufficient knowledge and awareness regarding the sensitivity of the information contained in electronic medical records which were regarded as the leading causes of security breaches in Amman's public hospitals. The study further revealed that no training or seminars were held to offer employees with fundamental understanding of the sensitivity of patient information and the security of electronic medical records, which were conducted in the hospital. The study did not explore the appropriate kind of training and seminars required and the main reasons for lack of training and seminar in the hospitals. The findings did not support the hypothesis of this study since examined the general information security issues not specifically to the influence of security awareness training on security of electronic health records, thus, it's findings may not necessarily be applicable to electronic health records.

The study conducted by Abuhammad et al. (2020) on the effect of user awareness on security controls found that awareness training had a substantial influence on practice of data-sharing and confidentiality in Amman hospitals in Jordan. The study concluded that as nurses' knowledge of information security controls increased, their confidentiality practices regarding patient data increased. The findings were consistent with those of (Khac Hai et al., & Karasneh et al., 2017), who discovered

that as nurses' and healthcare providers' knowledge of data sharing and confidentiality increases they exhibited greater confidentiality when sharing patients' data. The study concurred that insufficient security knowledge and skills among healthcare providers are the primary causes of improper data sharing practices and a lack of confidentiality in electronic health records. However, despite of their findings, the study did not explore the effects of training and awareness to other users apart from nurses like medical doctors, record officers, pharmacists and administrative officers which were the main focus of this study.

In a study on the effects of security awareness on the security of healthcare data by Nasser et al. (2020) it was discovered that healthcare staff who had not received security awareness training were more susceptible to phishing assaults because they had disregarded security issues. The results also showed that high patient-to-staff ratios, especially in developing nations, frequently result in healthcare providers being overworked and dealing with emergency situations at work. This increases their cognitive load and, as a result, makes them less aware of security controls. The study came to the conclusion that regardless of the nature of their jobs, users (administrative staff and clinicians) need to be educated on information security controls in order to practice digital hygiene in their daily work. This finding do not agree with the study hypothesis that security awareness training has no influence on security of electronic health records in the hospitals.

Another study undertaken by Saminu. (2019), on the effective information security management in healthcare organizations in Katsina, indicated that many healthcare providers lacked knowledge of securing electronic health records, especially when

sharing information between locations which contributed to security and privacy breaches of patient's data. Similarly, Stewart and Jurjens, (2017) noted that healthcare providers with inadequate security knowledge, training, and perception undermine better cyber security hygiene when phishing attacks occur. However, despite the fact that this finding do not support the current study hypothesis, the study findings did not mention specifically which kind of security awareness training employees lack in their hospital in order to strengthen its findings and hence be able to make comparisons.

Additionally, Khac et al. (2017) in their study on influence of nurse knowledge on data sharing found that as nurses and other healthcare providers' knowledge of data sharing and confidentiality increases, they demonstrated more outstanding commitment to patient data security. The study recommended on providing educational knowledge on data sharing and confidentiality as the most effective method for ensuring compliance with guidelines regarding security and privacy, also it was recommended that health organizations should frequently make all healthcare systems users up to date on the regulations and methods for stopping sensitive information disclosure. The study did not support the null hypothesis formulated in this but it focused on knowledge and awareness on data sharing and not awareness on security and privacy controls in general.

According to Kanani (2016) Tanzanian healthcare practitioners underutilize ICT resources when providing healthcare services because they lack ICT knowledge and skills particularly regarding security controls. The research findings indicate a lack of knowledge, proficiency, and awareness of ICT developments in health care services,

including security concerns with electronic health records (Busagala & Kawono 2013; Kanani 2016; Nehemiah, 2014). Additionally, Busagala and Kawono (2013a) demonstrated that the challenge is brought about by a lack of training, awareness-raising initiatives, and knowledge about the use of ICTs in the health sector (MOSHW, 2013), which results in an increase in security breaches

#### **2.4.2 Influence of Security Assessment on Security of Electronic Health Records.**

According to Schneier (2001), on security monitoring practices in organizations, the study found that security monitoring has a positive influence on security controls in organizations, the study argued that when security assessment conducted offers a real-time visibility of network security performance as it evolves in response to new attacks, emerging threats, software upgrades, and network reconfigurations. Similarly, Weidman (2014), supported this finding that security monitoring influence security controls in organization by providing real time responses. For instance, penetration tests examine the network's health for vulnerability scans. A vulnerability scan evaluates factors such as open ports and configurations to determine whether they provide the required level of security. Despite of this finding, the study did not specifically, examined the influence of security assessment in electronic health records.

In a study conducted by Wu et al. (2017) on secure controls for healthcare information systems found that the security monitoring practices influence security controls, the study mentioned the security audit log as substantially pertinent verification of security monitoring as it helps to reveal people who assessed the hospital information system, the information accessed and any changes made in the

systems if any. HIPAA (2015) is in consistent with Wu et al. as emphasizes that security audit trail logs must be kept following information storage principles and that all electronic applications that interface with EHR must fall within the audit trail's purview to alleviate the risk of security threats, data breaches, and fraud. Despite of this findings the results focused on few security controls assessment like audit log and less emphasis was put to other aspects of security controls assessment like vulnerability assessment, penetration test e.tc.

According to NIST (2017), security assessment is important in security controls as security assessment involves evaluating how an organization perform its routine security systems support and maintenance. The study revealed that when operating systems and software are regularly updated as needed, physical devices are cleaned, and physical infrastructure is monitored for damage all this influence effective security controls in organizations. It recommended that maintenance should be managed and performed on a regular schedule, or it can be unmanaged and performed off-schedule. The finding was about the influence of security assessment in general and not specifically on security of electronic health records hence, do not reflect this study purpose. The study concluded that lack of security assessment including systems maintenance can result into security and privacy breaches in an organization.

According to study by Kouns (2010), on evaluation of information security risk assessment for internet banking among commercial banks in Kenya, it was found that “security control assessments are applied to determine whether the system can maintain the security of the organization and whether the system and the

organization are able to respond appropriately in the event of a security breach. The study stated that the purpose of security control assessment is to identify which controls are malfunctioning or which areas of the network need to be further secured, and if existing security controls in place, they can be tested to see if they are effective. The study concluded that without security controls assessment it is difficult to determine which part of the information system is vulnerable to attackers or to identify why the system is not performing correctly in healthcare organizations. Despite this finding, the study was conducted in banking sector hence; its results might not reflect security of healthcare settings.

A study conducted by Aljumaili (2016) on data quality assessment applied in information system, found that security monitoring informs of quality assurance had a positive influence on security controls; it helps to stipulate better guarantee that the security measures implemented will protect their most valuable data from unauthorized changes, be accessible only to authorized parties and be available when needed. The study recommended that organization should adopt information security quality assurance rather than relying solely on auditors to evaluate their implemented security capabilities. Quality assurance will aid in providing prompt responses to management to assure them that information security controls meet their intended objectives (Clark, 2020). Despite this finding the study was not conducted in healthcare settings hence, its findings might not be applicable in health care environment.

The study by Fernando (2018), on standards for medical device cybersecurity, it was found that security monitoring important as it involves the assessment of the

implemented disaster recovery plan to guarantee business continuity and the availability of security controls in the occurrence of a disaster. The study asserts that disaster recovery and contingency plans may be implemented but neither IT nor other departments' personnel may be aware of their existence or the contents of the plan (Pumphrey, 2016). The study concluded that organization should implement contingency plan and provide staff with regular awareness training on implemented contingency plan so that they keep informed on organization's implemented contingency plan and how to use it. The study did not describe other security controls assessment in details hence do not support this study hypothesis.

According to the study by Rainie (2018), on internet of Things (IoT) security assessment for households found that in healthcare settings risk monitoring and security assessment has a positive effect on security controls. The study recommended that security assessment should be a standard part of an organization's operations, with periodic risk assessments to be conducted to determine the security footprint of the organization. Ayatollahi and Shagerdi (2017) supported the study by stating that risk assessment must be performed frequently and especially when additions are made to the network or new devices are installed. Further, the study stated that the new hardware or software may be the subject of a risk assessment to guarantee that adding the device, software, or individual to the network will not introduce an unacceptable level of unmitigated risk that can compromise the security control measures. Despite this finding the study focused on the security of Internet of Things and not electronic health records.



According to Jacobs (2016), study on security assessment it was revealed that the goal of risk monitoring and assessment is to detect relevant threats and vulnerabilities in an organization's inside and outside systems, the effect of a threat exploiting a vulnerability, and the probability of a threat occurrence. The study found that through security assessment healthcare organizations can increase their resilience by keeping secure and updated backups so that an attacks does not lead to the permanent harm to the healthcare data. The findings by Darzi and Kinross (2017) supported this finding that healthcare organizations should establish standardized security protocols and other strategies for improving the security of EHRs including the provision of relevant resources, the development of strategic plans for incident responses. The study finding did not focused on security of electronic health records rather it focused on broader range of security controls assessment in health information systems.

#### **2.4.3 Influence of Security Automation on Security of EHRs**

According to the study conducted by Jacobs (2016), on security controls assessment, the study found that security automation is part of security monitoring which is effective as many security functions are designed to be automated or have "set and forget" controls that are only occasionally fine-tuned. Antivirus software, for instance, is usually made to operate on a schedule or in reaction to certain events such as the insertion of a CD, USB flash drive, or email attachment. Additionally, emails are automatically scanned by the spam filters. The study found that systems have the ability to alert system administrators to questionable activity or to take appropriate action in response to it. For example, the system might notify the

administrator via email of a possible issue, or it might act independently and respond quickly. The study examines the impact of automation in security generally, rather than explicitly addressing the security of electronic health records.

According to the study carried out by Petters (2021), on security automation in cybersecurity found that security automation is powerful tool in security monitoring as it helps in ensuring instantly security controls. For instance, both intrusion detection systems and intrusion prevention systems automate security controls by monitoring network traffic and comparing the contents of packets to a database of known threats. The primary distinction between the two is that an intrusion detection system is a passive system that only performs detection and monitoring and does not act independently, in contrast intrusion prevention system is a control system that can drop malicious packets, (Petters, 2021). The study concluded that intrusion prevention systems are an excellent security controls as they can prevent incidents from occurring in the systems. Despite of its findings, the study did not focus on the influence of security automation on electronic health records hence do support this study hypothesis.

According to Capelo and Barbosa (2018), healthcare organizations must invest more in security automation systems, such as automatic audit logs and reviews of web applications that could pose growing security threats. More specifically, the study stated that “automated tools, including firewalls and antiviruses, as well as passwords and user credentials, cryptography and encryption, and IDS, are helpful in preventing or limiting access to patient data and in maintaining security controls. Additionally, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) stipulates

that despite of implementing of these automatic tools, healthcare organizations must regularly update automation tools to be up to date as the computers in hospitals and healthcare facilities are constantly under attack with new viruses. Despite of the findings, the study was carried out in developed nations hence its results might not fit the context of developing countries like Tanzania.

Similarly, automation techniques like audit logs, virtual private networks, tokens for user access, and access control lists are efficient ways for healthcare organizations to implement security controls, (Wanyonyi et al. (2017) on the effectiveness of security controls on electronic health records in Kenya. Bey and Magalhaes (2013) corroborated Wanyonyi's findings, which show that intrusion detection systems (IDS), cryptography, encryption, password and user name credentials, firewalls, and anti-virus software are useful automated controls for preserving system authentication. They claim that if the system allows for the encryption of patient data both in transit and at rest, then if attackers and cybercriminals gain access to the healthcare information system, it will be impossible for them to decode patient data.

The study by McAfee (2021) on security automation in cybersecurity stated that automatic monitoring such as endpoint detection and response is a form of security automation which can be implemented in an organization to enhance security controls. The study revealed that endpoint detection response combines real-time tracking and data capture with automated response, and analytics. The study recommends that integrating a high level of automation enables security teams to identify and respond to threats and vulnerabilities rapidly. The study concluded that automating endpoint security is critical in order to block attackers from accessing the

end point devices. Despite of this finding the study lack detailed description on influence of security automation on security EHRs in the health organizations.

The study by Kirtley (2018), on the effects of security vulnerability assessment stated that the use of vulnerability assessment software is an additional type of security monitoring which can be implemented in healthcare organizations to influence security controls. The study revealed that this software works within an IT environment to carry out many vulnerability checks, including patches that are missing or security configuration settings that are wrong rather than requiring a person to perform each check manually. The study recommended that specific approaches and tools need to be used to identify known or potential system vulnerabilities. The study further added that integrating vulnerability-detection products with other IT processes ensures that the entire security life cycle operates efficiently. The study was conducted outside of Tanzania healthcare settings hence it is findings do not reflect Tanzanian healthcare context.

The study conducted by Addy and Bala (2016) on physical access control based on biometrics, suggested using automated security tools like biometric authentication techniques in healthcare organizations in conjunction with multi-factor authentication for access to data in sensitive areas (such as server rooms/data centres and network termination rooms) increases the security of patient's data. Further, the study found that the use of biometrics in health care make it extremely tough, if not impossible, to forge an individual's identity (Smith, 2008). The study also added that biometrics have the potential to increase the security of the healthcare system by

limiting authorized access to a small number of individuals (Shank, Willborn, PytlikZillig, & Noel, 2012).

According to Tanzania Health Enterprise Architecture (2020), which is the document for guiding digital implementations in health services in Tanzania, healthcare organizations in Tanzania have not adequately automate its security controls. The paper suggests that the effective implementation of security automation in electronic health systems such as access management control, antivirus/anti-spam, desktop and enterprise firewall, email security, public key, intrusion detection and prevention, proxy server/directory services, secure data transport, and electronic fingerprinting as this technology results into an effective security controls in healthcare settings. The guideline mentioned that these techniques can be employed in a server and to the computers to protect the health information systems in healthcare services facilities during data processing, storage and on transit.

#### **2.4.4 Influence of Behavioural Monitoring on Security of EHRs**

A study by Calic et al. (2016) on Naive and accidental behaviours that compromise information security found that users' actions affect security controls in information systems. The study listed users' activities related to information systems security and privacy breaches, such as: Using unauthorized external media, sharing too much information on social media, accessing dubious websites, clicking on links carelessly, using the same password repeatedly, opening attachments from dubious sources, sending private information via mobile networks, owning personal electronics without physically securing them, and failing to update security software are all examples of risk behaviours in information system.

Despite of the finding the study did not focus on influence of behavioural monitoring to healthcare users particularly in electronic health records.

Balozian and Leidner (2017), in their study to identify the factors affecting the employee's behaviour of security compliance discovered that monitoring and evaluation were the critical determinants of employee compliance behaviour of the employees in terms of security compliance. More specifically the study revealed that when users in information systems feel that their activities are well monitored, they tend to comply to the security policies of an organizations. The study concluded that lack of user's behavioural monitoring results into employee's misbehaviour and inappropriate actions as it become impossible to identify their actions in the absence of these controls. The study assessed the factors affecting employee's behaviour of security compliance and not the influence of behavioural monitoring to security of electronic health records.

According to Veksler et al. (2018), in their study simulations in cyber-security: a review of cognitive modelling of network attackers, defenders, and users the study found that users of information system have the effects on security controls and therefore, for an organization to increase security controls the computer system users should use strong passwords, which makes usability completely difficult. The study stated that user's behaviour of choosing a weak password and using the same password for several websites should be discouraged for effective security controls in healthcare information systems. Sharing of passwords is a problematic for security controls as cybercriminals once get these passwords in one system, they normally apply these passwords in many other systems if are not effectively monitored (Martin

et al., 2012). The study finding did not focused on users behavioural monitoring rather if focused on type of users' behaviour which affect security controls.

According to the study by Maqbool et al. (2020), on cyber security: effects of penalizing defenders in cyber-security games via experimentation and computational modelling stated that users should be enforced on compliance in security controls by penalizing/ punishing users of information systems on misbehaviours in information system security controls, this can increase security compliance behaviours. The study described that with specific rewards and losses, security policies can be enforced more effectively. For example, healthcare organization must impose fines (kind of punishment learning) to all users/employees who do not comply to information security policies. The study concluded that when users are well trained that, what is expected is their adherence to the stated security policies and procedures they will obviously behave accordingly. The study recommended that if users fail to adhere to policies, punishments should be imposed according to the stated disciplinary actions.

According to Baillon et al. (2019), on their study on informing, simulating experience, or both: a field experiment on phishing risks found that users have a strong influence on security controls in organizations. The specifically study stated that providing users security awareness on behaviours influencing security breaches can influence the future impact on safe behaviours. Further, the study suggested that providing information on the average number of security breaches ("failures") increases the level of adherence to security policies among computer system users. The study concluded that when users are trained they get to think about the future consequences regarding security controls. Reflection is linked to future thinking and

planning, which can reduce impulsive behaviour, which is linked to risky behaviour on the security controls (Eskritt et al., 2014). Despite of the finding, the study did not focus on behavioural monitoring practices in electronic health records.

Rajivan et al. (2020) on their study on information security controls found that one of the most common errors in information security controls was users' behaviour of delaying or not installing security software updates at all. Most modern software systems are designed to automatically download and install security updates and other critical updates without human intervention. On the other hand, a manual update gives you more control over your device by choosing which update you want to install and when you want to install it. The study also located that risk-taking behaviours partly explain some people's behaviour concerning installing software updates. For example, more risk-averse people tend to delay installing software updates.

The results of a study conducted by Nehemiah, (2014) on "towards EHR interoperability in Tanzania hospitals: issues, challenges and opportunities" in three hospitals in Tanzania with 240 participants found that participants were concerned about users' behaviour which can results into security and privacy breaches of patient's information such as, hacking (79.5%), malicious software (69%) and unauthorized access (70%) as the most common threats to EHR systems. The study further revealed that the majority of hospital access violations are the result of users' behaviours or insufficient operational policies. For instance, one of his study's respondents reported that in one of the hospitals, during a field study, he was granted access to actual patient data, including names and medication details of patients.



Despite of findings, the study was conducted to access interoperability issues hence, less attention on the influence of behavioural monitoring on security of electronic health records in Tanzanian public hospitals.

#### **2.4.5 The Security Controls of Electronic Health Records**

The security goals of an information systems may be classified as availability, integrity and confidentiality. The confidentiality deals with who should access what in a system, integrity ensures no alteration of data from sender to receivers while availability ensures information is available to all intended users when needed.

##### **2.4.5.1 Confidentiality**

According to a study by Shamsi and Khojaye (2018), misconfigured information systems are the most common reasons for data loss in information systems. Information systems that are misconfigured are susceptible to injection flaws, including SQL injection, cross-site scripting, email injection, IMAP/SMTP injection and other attacks, as per OWASP, (2017). Lubis et al. (2018) stated that “Information System Security Misconfiguration is the Cause of Confidentiality Breaches. The study further asserted that attacks can bypass the system’s authentication and authorization. Spam Relay, Spam Injection (IMAP/SMTP) and Information Leakage. According to the study, “XPath injection attacks perform custom XPath queries inside the application to access unauthorized data and bypass authentication.

According to Liu and Kavakli (2018), information system restrictions on what validated users are permitted to do are frequently not enforced. They argued that this is one of the possible causes of information disclosure to unauthorized parties. Consequently, the information's confidentiality is compromised. They added that

confidentiality of the information is reliant on efficient security control measures and their appropriate settings and configuration to protect information during capture, processing, storage, and transmission.

According to the study by Sultan et al. (2018), physical layer end-to-end encryption can ensure confidentiality of information security. However, OWASP (2017) stated that information system design flaws render end-to-end encrypted information systems ineffective. Agrawal et al. (2018) claimed that sensitive data logs must be monitored and secured to increase confidentiality. Kolli et al. (2018) argued that system users and stakeholders should receive security education. Awareness should encompass the identification and implementation of effective security measures to protect the confidentiality of sensitive data during information states (capturing, processing, storage and transmission).

Gagneja (2017) proposes that healthcare facilities must install defence mechanisms and detection tools such as IDS (Intrusion Detection Systems) to protect against malicious attacks. Sittig (2016) suggests that healthcare institutions should develop monitoring systems to identify distrustful action including significant increase in network traffic, notifications of email messages from unidentified sources, and including executable files as an email attachment. According to Sittig (2016), healthcare institutions should implement encryption and decryption methods for electronic patient records (EHRs) on work systems and slides. All stored or transmitted EHRs must be encrypted. EHR encryption can protect health data and prevent listening and skimming.

#### **2.4.5.2 Integrity**

According to Baset and Denning (2017), numerous information systems are created without appropriate input authentications. The research contends that they allow invalid data inputs into the specified system. This can allow attackers to bypass authentication and authorization by injecting cross-site scripts and SQL injection into an information system. This causes a data integrity breach in the information system. This claim was backed up by the World Organization of Security Professionals OWASP (2017), which reported that information system misconfigurations and input validation (or “inspection” or “sanitization”) failures are the most common causes of SQL injection and CSR attacks. Injection flaws compromise the integrity of data/information in information systems, especially in healthcare systems.

Hermawan and Wardhani (2017) state that the usage of digital signatures can aid in maintain the security and integrity of data within systems. The study claims that using a digital signature correctly can ensure that data hasn't been changed by unauthorized users. Rezaighaleh also suggested using a time-based digital signature to thwart attempts to alter data. By using a digital signature, organizations can ensure that the communication is authentic and hasn't been altered in transit. Elkamchouchi (2018) proposed hybrid digital signature techniques for effective security measures.

#### **2.4.5.3 Availability**

Rudman (2014) posits that unavailability of information system can be attributed to natural disasters like floods, fires, storms or earthquakes as well as human acts like bombings or strikes, incorrect configuration of information systems, capacity resource limitations or outages. Similarly, Bosworth and Co. (2014) state that mail

spam blockers (like spamhaus) automatically blacklist spam-delivering mail systems when they send and receive emails from valid domains. Additionally, the research points to the possibility that injection attacks such as email (SMTP/IMAP) injection attacks may result in spam-delivering botnets and relays. This may prevent authorized users from accessing a mail system.

According to Chen and Chen (2017), denial-of-service (DoS/DDoS) attacks are the most common cause of information system (I2S) availability violations. The main causes of DoS / DDoS are injection attacks, which compromise an information system's operation and availability. Injection attacks, such as SQL injection or cross-site scripting (Cross-site scripting), can bypass authentication and authorization. This can compromise an entire information system. As a result, the information system is rendered inoperable. Ensuring the availability of information systems across all information states (capture, processing, storage, and transfer) is challenging.

According to the study by Gagneja (2017), "healthcare organizations should set up defence mechanisms and detection systems, such as intrusion detection systems (IDS), to detect malicious attacks. Sittig's and Singh's (2016) recommendations for monitoring systems include: Significantly increased network traffic Receiving emails from unknown sources Including executable files as attachments Encrypting and decrypting electronic data All stored or transmitted electronic health records (EHRs) must be encrypted on work systems and on slides. Encryption can be done in hardware and software (Serge, 2006).

According to Alhazmi's (2015), effective backup and testing restores ensure the availability of the information system. A business needs a business continuity plan

(BCP), system monitoring, event management and response (IMR) to guarantee the availability of information systems. In Mahimane's (2013) view, capacity planning encompasses determining the threshold, including bandwidth, performance and resilience requirements. According to Baruah (2013), hardware and infrastructure that is functional and has enough processing capacity to process all requests in a reasonable amount of time can ensure the availability of an IT system.

According to Sabena (2015), the availability of the organization's information system can be achieved through scheduled proactive maintenance as well as emergency maintenance of the information system components. For example, the availability of information system can be ensured by performing hardware repair as soon as it's needed and maintaining a software conflict-free operating environment. The availability of system can also be ensured by ensuring that there is enough communication bandwidth and that there aren't any bottleneck situations, as suggested by per (Line, 2015).

## **2.5 Policy Review**

The present national health policy in Tanzania created from Arusha declaration of 1967, the country's most national popular policy after independence. Health sector reform were instituted in 1993 as a result of a review that found that despite government efforts to implement the National Health Policy since the post-independence era, health outcome and impact indicators such as life expectancy, infant and child health, maternal health and other health indicators had remained poor. To embrace the use of eHealth as a solution to the present and future challenges in healthcare, the government, through the Ministry of Health, initiated a

comprehensive national health policy reform in the early 2000s. The Public Services Management and Employment Policy 1998, which was also released by the Tanzanian government, stipulated that public institutions must have robust M&E systems in place in order to address management issues and satisfy stakeholder requests.

The national policy specifically stated that all healthcare facilities should embrace the use of ICT in healthcare services delivery. The adoption and use of eHealth was achieved by the establishment of the national eHealth strategy (2013-2018), Health sector strategy plan IV (HSSP IV), Tanzania Digital Health Strategic Plan (2017-2023) and monitoring and evaluation strategic framework (MESF 2020-2025). To operationalize the adoption and use of electronic health records, the implementation strategy (National eHealth strategy 2013-2018) framework specified the need to have personal data protection act. Currently, the government have developed the personal data protection act, 2022 which established the minimum requirements for collection and processing of personal data. Unfortunately, the act is too general, there is still a lack of strong personal data protection act particular on electronic health records due to the sensitivity of patient's information.

Furthermore, the national eHealth strategy 2013-2018 provided a framework on adoption and implementation of eHealth, however according to Adebosina (2013) in the framework there was an absence of standards and systems interoperability which may threatens the security of electronic health records. Moreover, the national eHealth implementation strategy plan lacked a clear governance structure (Kajirunga & Kalegele 2015) which in one way or another hinder the monitoring of eHealth

including security monitoring practices. This observation recommends a greater focus on the review of the existing National Health Policy particularly eHealth policy, healthy M&E policy and other national implementation strategy to put more emphasises on security monitoring practices. This may improve security controls of patient's data and hence, increases confidence to patients when their information is kept in the health information systems.

## **2.6 Research Gap**

There has been a number of useful studies on the influence of security monitoring practices on the security controls, respondents have agreed that the security monitoring is a main contributor to security controls (Papoutsi et al., 2015; Meingast et al., 2006; Glassman et al., 2015; Alqahtani. & Braun. 2021). Though many studies carried out mainly dealt with the influence of security monitoring practices on security controls in general, there is inadequate studies which have focused specifically on the influence security monitoring practices on security of electronic health records in isolation and greater detail. Hence, there is a knowledge gap.

Moreover, the previous studies that have been carried out are mainly from USA, UK, Germany, Denmark, England, Australia, United Arab Emirates, South Africa, Egypt, Kenya and the like. There is a lacks of studies or little is known on the influence of security monitoring practices on security of EHRs from a Tanzanian hospital perspective. Furthermore, the studies which has been conducted on security of EHRs have not focused on security monitoring as one of the factor for security controls in electronic health records in Tanzanian hospitals (Busagala 2013; Nehemiah, 2014; Kajiruga, et al., 2015; Kanani, 2016; Freye et al., 2020). The gaps in the literature,

specifically the limited studies that detailed the influence of monitoring practices on security of EHRs in Tanzania motivated this study. There are limited theoretical understanding of the influence of security monitoring on security of EHRs, hence, creating a conceptual gap. Thus, to address this gaps, this research was carried to assess the influence of security monitoring practices on security of EHRs in Tanzania.

## **2.6 Conceptual Framework**

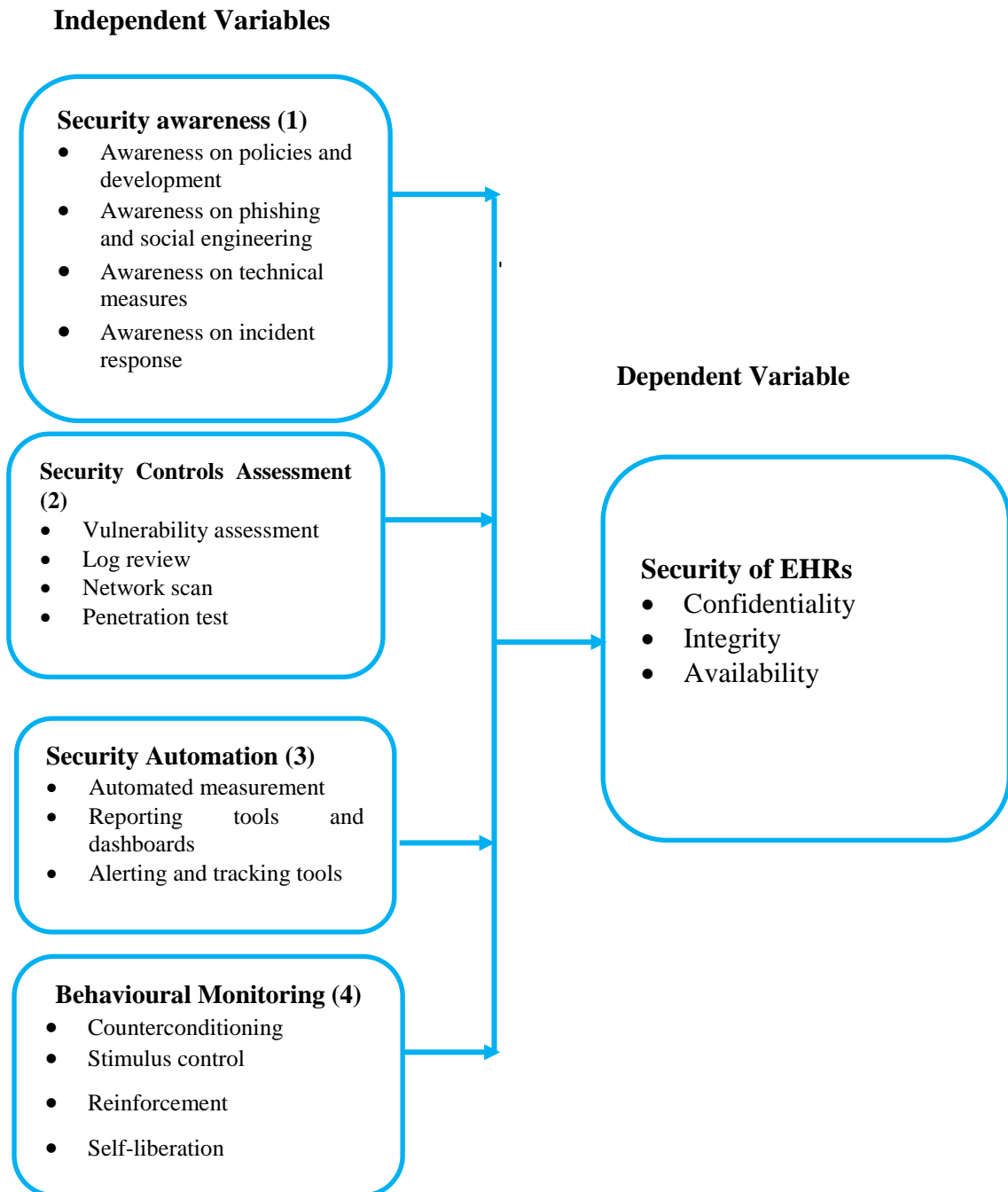
The independent variables of the study namely security awareness training, security assessment, security automation and behavioural monitoring have 15 variables. The dependent variable which is security controls of EHRs have three variables i.e. confidentiality, integrity and availability. Security awareness training constructs includes awareness on policies and its development, awareness on phishing and social engineering, awareness on technical measures and awareness on incident response. Security assessment constructs includes, vulnerabilities assessment, log review, network scan and penetration testing, security automation construct include automated measurement, reporting tools and dashboards and alerting and tracking tools. Behavioural monitoring comprises of constructs such as counterconditioning, stimulus controls, reinforcement and self-liberation.

The timely gathering, organization and analysis of security events generated from a wide range of network systems and applications deployed in their environment is one of the security management challenges that healthcare organizations are currently facing. Practices for security monitoring make it easier to be aware of threats and vulnerabilities over time and support managerial decisions on security measures



inside an organization. Healthcare businesses must evaluate information security risks and security controls frequently enough to enable risk-based decision-making inside the organization, as implied by the phrases continuous and ongoing. The results of security monitoring programs enable firms to take appropriate risk-reaction measures.

Healthcare management is able to make more informed and fast risk management decisions, including decisions about ongoing security authorizations when they have continuous access to security-related data via reports and dashboards. Automation makes it possible to update security authorization packages, inventories of hardware, software, and firmware, and other system data more often. When information from security monitoring is organized to be precise, quantifiable, actionable, pertinent, and timely, effectiveness is further increased. Information systems security categories determine how security monitoring procedures should be scaled (National Institute of Standards and Technology, 2013).



**Figure 2.1 Conceptual Framework**

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1 Chapter Overview**

The chapter addresses the methods and procedures used in the study. It shows how the research problem hinted in chapter one and two was approached and designed and how its supportive data were collected and analysed. These procedures and techniques, as also affirmed by Kallet (2004), offer a chance to the reader for critically evaluate a study's overall validity and reliability. Specifically, this chapter introduces the study design and study area along with the rationale of choosing the study areas, sampling design and generally methodological issues employed by the study. The applied methods produced the results and their discussion presented in chapters four and five, respectively. Finally, the results and their discussion obtained through such methods produced the summary, conclusions and policy implications addressed in chapter six.

#### **3.2 Research Philosophy**

The study's philosophy was grounded on positivist. The positivist philosophy focuses on the cause-and-effect opinion. This research philosophy was chosen because of the hypothesis to be tested. Positivism is characterized by the conviction that reality is constant and can be observed and depicted objectively without interfering with events (Matta, 2015). By investigating what actually occurs in organizations via the scientific measurement of people and behaviours, it is also possible to evaluate the hypotheses and generalize the findings (Halfpenny, 2015). The research was based on hypotheses that were developed, and logical and

empirical testing was done using quantitative methodologies. Positivism holds that events can be isolated and observations can be repeated, and it accepts that reality is constant and that it can be viewed objectively.

### **3.3. Research design**

A descriptive research design was used to establish the relationship between security monitoring practices and security of EHRs by explicitly testing the developed hypothesis. The cross-sectional research design was adopted. A cross-sectional research design is created to examine one aspect of a phenomenon at a time (Kumar, 2015). The researcher intended to learn more about the occurrence of an event or a scenario, phenomena, problem, state of mind, or topic under investigation, hence this design works well for the study. The findings from the cross-sectional approach are more generalizable to a population outside of the one under research than those from the case study design. Thus, in regard to this fact, the quantitative data was collected only once in the selected public hospitals to serve time and costs. The cross-sectional design was also significant for this research as it facilitated the researcher to ascertain the relationship between the independent and dependent variable of this study. Some advantages of this design it helps to serve time and it helps to display the association that exists among predictors and outcome variable.

### **3.4. Research Approach**

The study employed quantitative research approach. A quantitative research approach was selected to enable the testing of the hypotheses related with the proposed model (Mehrad & Tahriri, 2019). The quantitative research method properly suits the study focus because of the advanced ways of investigating,

explaining, and correctly scrutinising the factual inter-relational issues among multiple relationship dynamics of interest and also help in generalization of study findings (Creswell, 2014).

Functionally the quantitative method helps present findings from population samples where findings through outcome analysis and generalization apply to a larger population (Vogt, 2007). Making mathematical generalizations and performing a micro-analysis that stands up to a wide range (Stake, 2010). The purpose of quantitative methods is the conscious use of statistical data to generate research results (Creswell, 2014). In contrast, qualitative research techniques and comprehension processes are relatively flexible, allowing open-ended questions to interpret important patterns and isolate problems (Creswell & Poth, 2017). Given the fixed method required to solve a particular business problem, quantitative research methods are also based on closed structures of research and measurement using different data elements, including observational and performance channels to statistically interpret results and analyse hypothesis testing (Creswell, 2014).

### **3.5. Study Area**

This study was conducted in six public hospitals in Tanzania. The public hospitals selected were from each country zone as follows: Mount Meru Regional Referral Hospital in the Arusha Region in the Northern Zone, Temeke Regional Referral Hospital in the Dar es Salaam in the Eastern Zone, Dodoma Regional Referral Hospital in the Dodoma Region in Central Zone, Iringa Regional Referral Hospital in Iringa Region in the Southern Highland Zone, Sekou-Toure Regional Referral Hospital in Mwanza Region in the Lake Zone and Maweni Regional Referral

Hospital in Kigoma Region in the Western Zone. These hospitals were chosen because both were the first hospitals to adopt electronic health record systems and some of these hospitals were used for pilot study when the government was in the process of implementation of eHealth systems.

Furthermore, all of these hospitals are regional referral hospitals which have many departments with many employees and receive a large number of patients, hence necessitating a high level of ICT applications, particularly use of EHR systems and therefore, convenient for the researcher to get appropriate information on the influence of security monitoring practices on security of EHRs.

**Table 3.1 Description of Sampling Areas**

<b>SN</b>	<b>Name of hospital</b>	<b>Description</b>
1	<b>Dodoma Regional Referral Hospital</b>	It is a regional referral hospital located in Dodoma region in a central part of Tanzania, which was established in 1920. The hospital serves the Dodoma city population and its districts such as Kondoa, Kongwa, Mpwapwa, Chamwino and other neighbouring districts of Manyara and Singida regions. The hospital has implemented the use of EHRs in the delivery of health services since 2017.
2	<b>Iringa Regional Referral Hospital</b>	It is a regional referral hospital in the Iringa region in a Southern highland zone of Tanzania. The hospital is a referral hospital that receives patients from all districts of the Iringa region. The hospital has implemented the use of EHR in its health services delivery
3	<b>Maweni - Kigoma Regional Referral Hospital</b>	It is regional referral hospital of Kigoma region in Western zone of Tanzania. The hospital is serving Kigoma region populations and other districts of its neighbouring regions. The hospital has implemented the use of EHR in its health services delivery
4	<b>Mount Meru Regional Referral Hospital</b>	It is regional referral hospital located in the northern part of Tanzania in the city of Arusha. The hospital serves as a referral hospital for district hospitals and other health facilities in the Arusha region and nearby regions such as Manyara. The hospital is one of the earliest hospitals to use EHRs in health services delivery in Tanzania
5	<b>Sekou-Toure Regional Referral Hospital</b>	It is the regional referral hospital located in the Mwanza region in the Lake zone. The hospital serves as a referral hospital that receives patients from all districts of Mwanza region and its neighbouring districts of Mara and Kagera regions. The hospital is one of the earliest hospitals to use EHRs in health services delivery in Tanzania
6	<b>Temeke Regional Referral Hospital</b>	This is regional referral hospital located in Temeke district, in the Dar es Salaam region, in the Eastern zone of Tanzania. The hospital serves the Temeke population and its neighbouring districts of Mkuranga, Rufiji, Kisarawe and Ilala. The hospital is using EHRs in its health services delivery.

### **3.6. Target Population**

The target population of this thesis encompassed of EHR users in public hospitals such as IT officers, medical doctors, record officers, pharmacists, health laboratory technologists, nurses and administrative staff. The number of staff in this categories

which make the target population of this study was 1200, (Source, hospital's workers statistics).

### **3.7. Sampling Design and Techniques**

According to McCall (2018), sampling is selecting a small subset from the entire population. The sampling process is therefore, an important procedural element of study design to ensure that the sample is unbiased and accurately represents the entire population of interest. Preferably, sampling for quantitative studies is done using random sampling methods from large populations to constitute samples with similar characteristics in the same proportions as the entire population (Creswell & Creswell, 2017).

This study applied purposive and random sampling techniques. The purposive sampling was employed to select the six public hospitals. Each hospital was selected based on its longevity and experience on using electronic health records in its respective country zone. In the second stage, purposive sampling technique was also used to select a sample of respondents (IT officers, medical doctors, record officers, pharmacists, health laboratory technologists, nurses and administrative staff) within the selected public hospitals. Then, a simple random sampling technique was used to sample participants from the targeted population because the whole population under the study was accessible. From the targeted population, each member was assigned a number and a lottery method was used to determine which subjects were to be included in the sample, as proposed by Elfil and Negida (2017). This technique is recommended as it gives equal chance for each unit to be selected (Creswell, 2014).



Also, the sample which is selected using this method are more representative of the target population (Creswell, 2014).

Both of the selected public hospitals were in the same category, based on the Ministry of Health, healthcare facilities categorization, i.e., Regional Referral hospitals. Therefore, the number of staff in this targeted population was almost the same in each hospital. Yamane's formula (1967) was used to determine the sample size for this study. Using this formula, sample sizes can be calculated using precision levels of 0.03, 0.05, 0.07, and 0.01 (e).

Based on the study sampling frame, the sample size was computed at precision level of 5% (e = 0.05) as shown in equation 1 below:

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

Whereas:

n = Sample size for population.

N= Size of population

e= level of precision (0.05).

According to the above formula, the sample size for this study is: -

$$n = \frac{1200}{1 + 1200(0.05 \times 0.05)}$$

$$n = \frac{1200}{4}$$

$$n = 300$$

Thus, the minimum sample size for this study was 300 participants

**Table 3.2 Sampling frame**

<b>Regional Hospital</b>	<b>Population</b>	<b>Percent</b>	<b>Sample Size</b>
Dodoma	203	16.9	51
Iringa	190	15.8	48
Maweni	199	16.5	50
Mount Meru	208	17.3	52
Sekou Toure	206	17.1	52
Temeke-Dar es Salaam	194	16.1	49
<b>Total</b>	<b>1200</b>	<b>100</b>	<b>300</b>

Source: Researcher, 2022

### 3.8. Variables Measurement

The study measured respondents' opinions and perceptions quantitatively using a five-point Likert like scale (1-5), as proxy indicators reflecting respondent's perceptions and attitudes towards influence of security monitoring practices on security of EHRs. The scale provided a structured framework for respondents to express their levels of agreement or disagreement with the statements related to influence of security monitoring on security of EHRs in the hospitals. Willits, Theodri, and Luloff (2016) performed an extensive analysis of the Likert-point scale to account for several factors, such as the number of response categories that need to be presented, and the analysis and importance of response data. Their results finalize the overall structure, recommending that the practical number of items on the Likert scale be between 5 and 7, with greater than 4 scales increasing confidence measures and creating internal consistency (Willits et al, 2016). A detailed explanation of how the variables were measured using quantitative approaches are provided in the subsequent section.

### **3.8.1 The Dependent Variable**

The dependent variable of interest in this study was security controls of electronic health records which comprises confidentiality, integrity and availability. This is the outcome which healthcare organizations intend to achieve in goals of keeping patient's health record safe. In this study, three dimensions of security controls in electronic health records were assessed. These dimensions of the security controls are confidentiality, integrity and availability. Security controls in electronic health records were measured using quantitative approaches, which are explained in the subsequent paragraphs.

Table 3.3 summarizes and presents the approach and measurement used to assess security of electronic health records, i.e., the dependent variable of this study. The security controls were measured using three summary measures: Confidentiality, integrity and availability (Altaf et al., 2016). It was assessed using 16 Likert-type statements or items covering three dimensions of security controls in an organization.

The scale was converted into total scores, whereby the five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) from confidentiality ranged from a minimum of 5 to a maximum of 25 scores. Under integrity the five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) was converted into total scores, whereby six statements had a minimum of 5 to a maximum of 30 scores while in availability five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) resulted into minimum of 5 to a maximum of 25 scores.

**Table 3.3 : Dependent Variable Measurement**

Variable	Construct	Specific measurement
Security Controls	Confidentiality	CFD1: Encryption of sensitive data
		CFD2: Management of data access
		CFD3: securely dispose of data
		CFD4: Management of devices
	Integrity	IGT1: Data entry controls
		IGTC2: Data quality checks
		IGTC3: Audit trails and logs
		IGTC4: Regular backup and recovery
	Availability	ABT1: Continuity plan
		ABT2: System backups
		ABT3: System maintenance
		ABT4: Monitor availability

Source: Researcher, 2022

### 3.8.2 The Independent Variables

The independent variables comprise of four variables. These variables include, security awareness training, security control assessment, security automation and behavioural monitoring. The variables were measured using quantitative approaches. The five-point Likert scale ranging from 1 strongly disagree to 5 strongly agree was employed to measure the items of the variables in the surveyed public hospitals.

Security awareness training is a non-metric variable measured using ten items taken from the previous studies. The five-point Likert scale ranging from 1 strongly disagree to 5 strongly agree was used to measure the items of the variables in the surveyed public hospitals. Security controls assessment was a non-metric variable measured evaluated using eleven items obtained from the previous studies. These items are illustrated in table 3.4. The five-point Likert scale ranging from 1 strongly disagree to 5 strongly agree was used to measure the items of the variables in the surveyed hospitals.

Security automation was a non-metric variable measured using nine items obtained from the previous studies. The five-point Likert scale ranging from 1 strongly disagree to 5 strongly agree was used to measure the items of the variables in the surveyed public hospitals. The behavioural monitoring was a non-metric variable evaluated using eight items from the previous studies. The five-point Likert scale ranging from 1 strongly disagree to 5 strongly agree was used to measure the items of the variables in the surveyed public hospitals.

The scale was converted into total scores, whereby the five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) from security awareness ranged from a minimum of 5 to a maximum of 50 scores. Under security controls assessment the five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) was converted into total scores, whereby eleven statements had a minimum of 5 to a maximum of 55 scores while in security automation five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 Strongly agree) resulted into minimum of 5 to a maximum of 45 scores and behavioural monitoring five-point Likert scale (1 strongly disagree, 2 disagree, 3 somehow agree, 4 agree and 5 strongly agree) converted into total scores where by eleven statement had a minimum of 5 to a maximum of 55 scores.

**Table 3.4 : Measurement of independent variables**

Variables	Construct	Specific Measurement
Security awareness training	ISA	ISA1: Awareness on policies and development ISA2: Awareness on phishing and social engineering ISA3: Awareness on technical measures ISA4: Awareness on incident response
Security controls assessment	SCA	SCA1: Vulnerability assessment SCA2: Log review SCA3: Network review SCA4: Penetration test
Security automation	SAT	SAT1: Automated measurement SAT2: Reporting tools SAT3: Reporting tools
Behavioural Monitoring	BM	BM1: Counterconditioning BM2: Stimulus control BM3: Reinforcement BM4: Self-liberation

Source: Researcher, 2022

### 3.9. Data Collection Methods

The study gathered both primary and secondary data. The necessary quantitative data was collected using the survey questionnaire. With the use of the survey questionnaire, bias in data collection was prevented, costs were reduced, a big sample was contacted at a time, and as a result, the results were extra trustworthy and reliable (Kothari, 2004; Cohen et al., 2007; Saunders et al., 2009). This method's primary drawback is its low percentage of returned properly completed questionnaires due to inherent rigidity caused by the challenge of making changes to the approach after the questionnaire has been sent out. Because of these drawbacks,

the researcher tested the questionnaire in a pilot study before employing this approach (Cohen et al., 2007; Saunders et al., 2009).

Structured questionnaire was distributed anonymously to 360 respondents, and online data collection software (i.e., Kobo toolbox) was employed to collect data. To guarantee high level of confidentiality and retain the integrity of collected data, the survey link was sent to each participant personally through email address or their mobile phone. Respondents was requested to fill the consent declaration to have permission to start filling the survey.

The survey questionnaire (Appendix I) was created using the experiences gained from past related research surveys. A portion of the questions were created by incorporating the findings of prior studies and reviewing relevant literature (Ismail et al., 2010; Shaaban, 2014; Educause.edu, 2015).

### **3.9.2 Pilot Testing**

After the questionnaire was created and developed, a pilot study was carried out to evaluate the reliability and validity of the research instruments. Additionally, as mentioned by Pallant (2005), this test confirmed that the questions, instructions and scale items were clear. According to Cooper and Schindler's (2006) and Mugenda and Mugenda's (2003) study, a pilot study should include a sample of at least 10% of the target population. As a result, thirty (30) copies of the questionnaire set were dispersed at random to the participants who were chosen at each hospital under study. Pallant (2005) states that whenever possible, pilot test should be used on the same type of people to be involved in the main study. This was in consistent with (Sanders, Lewis & Thorhill, 2003; Fink, 1955) who stated that the number of

participant for the pilot test should be the same with the one to be involved in the study and should sufficient enough.

During pilot testing participants were requested first to fill out a questionnaire and then to provide comments on the questionnaire. Comments made were based on the nature of the question, the setting of the questions, and the ambiguity within the question. Comments received on readability, relevance, wording and comprehension were carried over to the second version of the survey and re-filled with some of the previous respondents. The comments were integrated and the final edition of the questionnaire was created. The final version produced a Cronbach's alpha of 0.864 implying that the tool was suitable for data collection.

### **3.10. Data Processing Methods**

According to Huang (2019), data processing refers to extracting information by organizing, indexing, and manipulating data. Data processing and analysis are important to guarantee that all pertinent data are acquired for the expected comparisons and analyses Mugenda (2008). In this study, variables were measured using Likert score with 5-items. From 1 strongly disagree to 5 strongly agree. Raw data collected during the data collection process were transformed into information to validate research hypotheses. Therefore, the collected information was organized, edited and coded before data analysis



**Table 3.5 Data Processing Matrix**

<b>Variables</b>	<b>Description</b>	<b>Measurement</b>	<b>Interpretation of Means</b>
<b>Security controls of EHRs</b>	<b>15 items</b>	<b>Score 15 – 75</b>	<b>If M=15-32 Low; 33-75 High</b>
Confidentiality	5 items	Score 5-25	If M=5-14.9 Low; 15-25 High
Integrity	5 items	Score 5-25	If M=5-14.9 Low; 15-25 High
Availability	5 items	Score 5-25	If M=5-14.9 Low; 15-25 High
<b>Security Awareness</b>	<b>10 items</b>	<b>Score 10 – 50</b>	<b>If M=10-27 Low; 28-50 High</b>
Awareness on policies and development	3 items	Score 3 – 15	If M=3-7.9 Low; 8-15 High
Awareness on phishing and social engineering	3 items	Score 3 – 15	If M=3-7.9 Low; 8-15 High
Awareness on technical measures	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
Awareness on incident response	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
<b>Security assessment</b>	<b>11 items</b>	<b>Score 11 – 55</b>	<b>If M=11-24 Low; 25-55 High</b>
Vulnerability assessment	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
Log review	3 items	Score 3 – 15	If M=3-7.9 Low; 8-15 High
Network review	4 items	Score 4 – 20	If M=4-9.9 Low; 10-20 High
Penetration test	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
<b>Security Automation</b>	<b>9 items</b>	<b>Score 9 – 45</b>	<b>If M=7-20 Low; 21-45 High</b>
Automated measurement	4 items	Score 4– 20	If M=4-9.9 Low; 10-20 High
Reporting tools	3 items	Score 3 – 15	If M=3-7.9 Low; 8-15 High
Alerting and tracking tools	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
<b>Behavioural Monitoring</b>	<b>8 items</b>	<b>Score 8 – 40</b>	<b>If M=7-20 Low; 21-40 High</b>
Counterconditioning	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
Stimulus control	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
Reinforcement	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High
Self-liberation	2 items	Score 2 – 10	If M=2-4.9 Low; 5-10 High

### **3.11 Data Analysis Methods**

In this study, data were analysed with the use of descriptive statistics analysis and inferential statistics analysis whereby correlation analysis and regression analysis were performed under inferential statistics. According to (Mbweza 2006; Mugenda & Mugenda 2003), descriptive analysis involves finding numerical summaries that present greater insight into the properties and explanations of the variables under study. The study used correlation analysis to determine if relationship between two or more variables exists. The amount and path of correlation are displayed by the correlation coefficient (Cohen et al., 2013). The dependent variable is assumed to be predictively related to the independent variable. Regression analysis therefore attempts to predict values of a continuous interval or scaled outcome variable from given values of the predictor variables.

Both statistical analysis which are descriptive statistics and inferential statistics was conducted with the use of Statistical Package for Social Sciences (SPSS) version 25 software. SPSS was chosen as it is easy to use and provides all the analysis needed, (Castillo, 2009). Response categories were identified, coded, and entered into the SPSS variables datasheet for descriptive and quantitative analysis. Descriptive analysis produced measures of central tendency such as frequencies, percentages, means and standard deviations which were displayed in tables and interpreted accordingly.

A conditional multiple linear regression test was performed to test the assumptions before further analysis of the data. These tests were the sample sufficiency test to examine the suitability of the sample size for factor analysis, the autocorrelation test

to determine if there is a correlation between the residual terms of any two observations, the multicollinearity test to test if two or more independent variables are correlated, the outlier test to determine if there are observations significantly different from other observations, the Bartlett test to determine if the correlation matrix is identity, and the normality test to determine if the data are normally distributed. After performing diagnostic tests, factor analysis was performed to identify factors that may not be relevant to the study. Finally, the researcher performed the correlation and regression analysis for the study (Babbie et al., 2007).

### **3.11.1 Sampling Adequacy Test**

The study employed the Kaiser-Meyer-Olki (KMO) method to assess the appropriateness of the sample size. KMO is a measure used by Magd (2008) to evaluate and support the appropriateness of applying factor analysis; values between 0.5 and 1.0 denote a significant factor. According to Moutinho and Hutcheson (2010), factor analysis works best with values between 0.7 and 0.8.

### **3.11.2 Autocorrelation Test**

An autocorrelation test was run in this study to check for any association between any two observations' residual terms. For any two observations, it is anticipated that the residual terms will be independent (Field, 2005; Levine, Fustephan, Krehbiel, & Berenson, 2004). A Durbin-Watson test was performed to test for autocorrelation between variables. The study by Gujarati (2003) found that the Durbin-Watson statistic ranges from 0 to 4. Values close to 0 indicate positive autocorrelation and values close to 4 indicate negative autocorrelation. A value between 1.5 and 2.5

denotes no autocorrelation. The detailed result on autocorrelation test are displayed in appendix ii.

### **3.11.3 Multicollinearity Test**

The study performed a multicollinearity test. Bickel (2010) found that in multiple regression models, multicollinearity happens in statistics where two or more independent variables are greatly correlated. The Gauss-Markov assumption simply necessitates that perfect multicollinearity is not present, and the model will be identified unless there is perfect multicollinearity. This implies that the model can estimate all coefficients, the coefficients remain the best linear unbiased estimates, and the standard errors are correct and efficient (Runkle et al., 2013). In this study, the Variance Inflation Factor (VIF) was used to examine multicollinearity problems in multiple regression. VIF statistic for the predictors in the model is the inverse of the error tolerance, which shows how large the error variance is relative to the predictor's intrinsic effects (Baguley, 2012).

According to Cohen & Cleveland (2013), the variance inflation factor (VIF) measure the amount by which the variance of each regression coefficient rises in comparison to the situation where all predictors are uncorrelated. As a rule of thumb, a VIF of 5 or more is used to conclude that the VIF is too large to be suitable. According to Runkle et al. (2013) if two or more variables hold a variance inflation factor (VIF) greater than or equal to 5, one should be eliminated from the regression analysis to indicate the existence of multicollinearity. Therefore, in this study, if more than one variable has a variance expansion factor of 5 or more than 5, one was eliminated

from the model. The detailed result on multicollinearity test are displayed in appendix ii.

#### **3.11.4 Normality Test**

The normality test was done to ascertain whether the data were well patterned and normally distributed (Gujarati, 2002). As Ghasemin and Zahediasi (2012) show, variables should be approximately normally distributed, particularly if you want to generalize results across samples. Both the Kolmogorov-Smirnoff normality test and the Shapiro-Wilk normality test were used in this study. A normality test value of less than 0.05 for the Kolmogorov-Smirnov test indicates that the data are not normally distributed. However, the data were normally distributed when the Shapiro-Wilk test result was less than 0.05. The detailed result on normality test are displayed in appendix ii.

#### **3.11.5 Factor Analysis**

The factor analysis was performed to examine variables that were statistically significant to the study. Shenoy and Madan (2000), contended that not all variables in studies are statistically significant. Factor analysis serves as a measure of the underlying significance of a particular variable to a factor it has been used to detect and eliminate hidden components or variables that do not meet research objectives and are not apparent in direct analysis (Ledesma & Valero-Mora, 2007; David et al., 2010). Commonality and eigenvalues were used to indicate the net importance of the variable factors. A burden value of 0.7 is a rule of thumb and is considered satisfactory, but there are obvious difficulties in meeting the 0.7 criterion, so a burden value of 0.4 is allowed (Rahim & Magna, 2005). In this study, the

eigenvalues of each strong indicator within the variables were extracted by the use of principal component analysis. The results on factor analysis are displayed in appendix iii of this study.

### **3.11.6 Correlation Analysis**

The significance and direction of the association between the outcome and predictor variables were examined in this study using Pearson's correlation coefficient. Values of the correlation coefficient ranging from -1 to +1. A correlation coefficient of +1 indicates that the two variables are perfectly connected in a positive linear sense, meaning that one variable grows as the other decreases (Neuman, 2006; Sekeran, 2008; Kothari, 2012; Collis & Roger, 2013). A value of 0 indicates that there is no relationship.

### **3.11.7 Regression Analysis**

Multiple linear regression analysis techniques were used as an inferential statistical technique to analyse quantitative data. The analysis was suitable for determining the relationship between the one dependent variable and many independent variables (Hair et al., 2014). Also, multiple linear regression analysis is appropriate for assessing the significance of each independent variable to a relationship (Tabachnick & Fidell, 2014). In these analyses, the dependent variable was security of EHRs and independent variables were security awareness training, security controls assessment, security automation and behavioural monitoring.

Security controls is said to be effective if it ensures confidentiality, integrity and availability of information. The security controls in electronic health records is directly proportional with security monitoring practices (FFIEC, 2006). Thus, to capture the

influence of security monitoring practices on security of electronic health records the equation 1 was used;

$$SCEHR = f(SM) \dots \dots \dots (1)$$

Whereby, SEHR=Security controls of EHRs, SM= Security monitoring

SCEHR is an index that was computed through the summation of all the variables of structural elements of security controls (SC) and structural elements of security monitoring (SM).

Since security monitoring is composed of SAT, SCA, SAUT and BM, therefore the following equations may be combined to form multiple linear regression model as presented in equation 2-6.

$SAT =$

$$\beta_0 + \beta_1 APD + \beta_2 APSE + \beta_3 ATM + \beta_4 AIR + \varepsilon_i \dots \dots \dots (2)$$

Whereby, SA= Security awareness training,  $\beta_0$  = Constant Term, APD = Awareness on policies and development, APSE= Awareness on phishing and social engineering, ATM= Awareness on technical measures, AIR=Awareness on incident responses and  $\varepsilon$  = Error Term

$$SCA = \beta_0 + \beta_1 VA + \beta_2 LR + \beta_3 NR + \beta_4 PT + \varepsilon_i \dots \dots \dots (3)$$

Whereby, SCA= Security controls assessment,  $\beta_0$  = Constant Term, VA = Vulnerability assessment, LR= Log review, NR= Network review, PT=Penetration test and  $\varepsilon$  = Error Term

$$SAUT = \beta_0 + \beta_1AM + \beta_2RTD + \beta_3ATT + \varepsilon_i \dots \dots \dots (4)$$

Where, SAUT= Security automation,  $\beta_0$  = Constant Term, AM = Automation measurement, RTD= Reporting tools and dashboards, ATT= Alerting and tracking tools and  $\varepsilon$  = Error Term

$$BM = \beta_0 + \beta_1CC + \beta_2SC + \beta_3RC + \beta_4SL + \varepsilon_i \dots \dots \dots (5)$$

Whereby, MB= Behavioural monitoring,  $\beta_0$  = Constant Term, SC = Counterconditioning, SC= Stimulus control, RC= Reinforcement, SL=Self-liberation and  $\varepsilon$  = Error Term

Combining the equation 2-5, resulted into equation 6 which was used in multiple linear regression analysis

$$EHRsc = \beta_0 + \beta_1SAT + \beta_2SCA + \beta_3SAUT + \beta_4BM + \varepsilon_i \dots \dots \dots (6)$$

Whereby;

SC = Security controls of EHRs

$\beta_0$  = Constant Term

$\beta_1$ = Beta coefficients

ISA= Information security awareness

SCA= Security controls assessment

SAUT= Security automation

BM= Behavioural monitoring

$\varepsilon$  = Error Term



### **3.12. Validity and Reliability**

#### **3.12.1 Validity**

The capacity of an instrument to measure what it is anticipated to measure is known as validity. Kumar (2005), mentioned the two approaches to determining the effectiveness of research instruments. Logical and statistical evidence. In this study, validity was determined by logical connections between questions and objectives. There are three aspects to checking validity. These include content, structure and adequacy of criteria (Orotho, 2009). Validity of the content was guaranteed by designing the tool in respect to the study variables and respective metrics. The validity of the constructs was maintained by limiting the question to the conceptualization of the variables and guaranteeing that the metrics for a given variable fit within the same construct.

Moreover, a pilot study was undertaken to establish robustness of the data collection instrument. Questionnaire were administered with 30 respondents from the selected six public hospitals. During pilot testing respondents were requested first to fill out a questionnaire and then to provide comments on the questionnaire. Comments made were based on the nature of the question, the setting of the questions, and the ambiguity within the question. Comments received on readability, relevance, wording and comprehension were carried over to the second version of the survey and re-filled with some of the previous respondents. The comments were integrated and the final edition of the questionnaire was created.

### 3.12.2 Reliability

Kothari (2014), portrayed that reliability is the ability of research tools to produce consistent results when repeated measurements are made in the same way. Cronbach's alpha was utilised in the study. This test was performed to conveniently determine the internal consistency or reliability of a composite score. Good, better, and best Cronbach's alpha values are 0.70, 0.80, and 0.90, respectively. As a result, the study decided on a cut-off point of 0.70 because 0.8 was beyond the established threshold. The findings of the reliability test are displayed in Table 3.6.

The reliability test was performed to measure the internal consistency of study findings. A reliability analysis was performed to compute Cronbach's alpha, as the results sufficiently tested the survey scale and obtained a reliability score (Sikaran & Bogie, 2016). Cronbach's alpha ( $\alpha$ ) in the 0-1 range indicates high values linked with improved reliability and internal consistency. George & Malley (2016) provide guidelines that reflect: 0.50 to 0.59 is poor, 0.60 to 0.69 is questionable, 0.70 to 0.79 is acceptable, 0.80 to 0.89 is good, and 0.90 to 1 is excellent. On the other hand, Cronbach's alpha coefficient has no real lower bound (Cronbach, 1951). Gliem & Gliem (2003) point out that higher alpha values reveal internal consistency of scales, but no indication of unidimensionality when factor analysis methods provide dimensionality of scales.

**Table 3.6 Summary of Reliability Test**

<b>Composite variable</b>	<b>Cronbach's alpha</b>	<b>Comments</b>
Security awareness training	0.740	Reliable
Security controls assessment	0.751	Reliable
Security automation	0.745	Reliable
Behavioural monitoring	0.725	Reliable

The results of the survey indicate that the construct scores range from  $> 0.7$  acceptable to  $> 0.9$  excellent. Table 3.6 above summarises the construct's internal consistency and reliability, indicating each variable and the particular ( $\alpha$ ) score and guideline level of consistency which revealed that each variable had 0.7 and above hence reliable.

### **3.13. Ethical Consideration**

While conducting this research study, all procedures and activities were directed by ethical considerations. Among the most critical precautions taken is the request for a clearance letter from the OUT's research and publication section. Other ethical considerations involved the confidentiality of the gathered data, which was certified by the researcher's signature on the OUT postgraduate directorate's declaration of confidentiality form. Additionally, the researcher obtained respondent's consent and kept consent forms as evidence. Furthermore, all processes of sample selection were governed by the principles of gender parity and equality.

## **CHAPTER FOUR**

### **RESEARCH FINDINGS**

#### **4.1 Chapter Overview**

This chapter presents the study findings after data analysis. It describes how the findings of the analysed quantitative data were presented in the study. The findings are presented based on each specific objective. The results presented about the influence of information security monitoring practices on security of electronic health records in Tanzanian public hospitals. The objectives were derived from chapter one and supported by the theories, empirical studies and logical relationships presented in chapter two. The objectives were guided and achieved using the methods presented in chapter three of the study. The interpretations, meanings and details of the obtained findings are discussed in chapter five which in turn led to the formulation of summary, conclusions, recommendations and implications of the study addressed in chapter six.

#### **4.2 Respondent's Demographic Description**

The demographic features of participants were not part of the study objectives but are displayed for the benefit of the readers to get some background information about the respondents involved in the study. Thus, the study presents the demographic characteristics of respondents involved regarding their gender, age group, education level, working experiences, occupations and working place. The gender results of the surveyed respondents indicated that 158(52.7%) were males and 142(47.3%) were females. Regarding the age group of respondents, the result revealed that 121(40.3%) was the age group between 20-30 years, 112(37.3%) was the age group between 31-

40 years, while 41(13.7%) was in the age group between 41-50 years, 26(8.7%) was in the age group between 51-60 years and none of the respondents was above 61 years.

The results on educational level of respondents established that 155(51.7) hold a bachelor's degree, 84(28%) had a diploma as their highest level of education, 43(14.3%) had a certificate and 18(6%) had a master's degree level of education, none of respondent had attained PhD. The results on occupations of respondents indicated that 26(8.7%) was IT officers, 68(22.7%) was medical doctors, 71(23.7%) was nurses, 56(18.7%) of respondents was pharmacists, 42(14%) was health laboratory technologists, 21(7%) was record officers and 16(5.3%) was administrative officers.

Furthermore, regarding variables on working experience, the range of experience was from less than 1 year to more than five years. The results indicate that 147(49%) had more than 5 years working experience; 100(33.3%) had 1-5 years of experiences; 41(13.7%) had 1-3 years of experiences and 12(4%) had less than 1 year of working experience. Thus, this result indicates that majority had more than 5 years of experience in the hospital. The result on respondent's working hospitals showed that 59(19.7%) of respondents were working at Mount Meru Regional Referral hospital, 54(18%) were working at Maweni Regional Referral hospital, 52(17.3%) were working at Iringa Regional Referral hospital, 46(15.3%) were working at Dodoma Regional Referral hospital, 45(15%) were working at Temeke Regional Referral hospital and 44(14.7%) they were working at Sekou-Toure Regional Referral hospital.

**Table 4.1 Sample Description**

<b>Variables</b>	<b>Category</b>	<b>Frequencies</b>	<b>Percentages</b>
Gender	Male	158	52.7
	Female	142	47.3
	<b>Total</b>	<b>300</b>	<b>100.00</b>
Age group	20-30	121	40.3
	31-40	112	37.3
	41-50	41	13.7
	51-60	26	8.7
	<b>Total</b>	<b>300</b>	<b>100.00</b>
	Education Level	Certificate	43
Diploma		84	28
Bachelor degree		155	51.7
Master degree		18	6
PhD		00	00
<b>Total</b>		<b>300</b>	<b>100.00</b>
Occupations	IT Officers	26	8.7
	Doctors	68	22.7
	Nurses	71	23.7
	Pharmacists	56	18.7
	Lab. Technologists	42	14
	Record officers	21	7
	Administrative officers	16	5.2
	<b>Total</b>	<b>300</b>	<b>100.00</b>
Working Experiences	Less than 1 year	12	4
	1-3 years	41	13.7
	1-5 years	100	33.3
	More than 5 years	147	49
	<b>Total</b>	<b>300</b>	<b>100.00</b>

---

Source: Researcher, 2022

### **4.3 Descriptive Statistics**

This part involves the assessment and description of the features of variables such as median, mode, mean scores, standard deviation, normality and possible outliers. The predictor variables used in this study included security awareness training, security controls assessment, security automation and behavioural monitoring. The respondent's perceptions were classified as high security or low security.

Before undertaking descriptive analysis on the influence of security monitoring practices on security of electronic health records, normality tests were conducted on the composite scores of security awareness training, security controls assessment, security automation and behavioural monitoring variables. Quantile-Quantile (Q-Q) plots and normal distribution plots were used for this assessment, both indicating a normal distribution pertaining to the data. Moreover, central tendency metrics, precisely mean, mode, and median, were computed to confirm their similarity, with the expected results if the data are normally distributed. The results exhibited that all composite score variables associated with independent variables of this study demonstrated a normal distribution (See detail in appendix ii figure 4.6-figure 4.8). Based on the assumption of a normal distribution, parametric tests like ANOVA was applied. The composite score which are all scale variables were classified based on the composite scores interpretation matrix devised in Table 3.5.

### 4.3.1 Descriptive Statistic for Security Awareness Training

The descriptive analysis findings indicated that all composite score variables associated with security awareness training demonstrate a normal distribution as detailed in appendix ii Figure 4.6 and Table 4.2. The composite score which are all scale variables were classified based on the composite scores interpretation matrix devised in Table 3.5.

**Table 4.2** Key descriptive statistics for security awareness training

Variable	Measure of central tendency					Security classification
	Mean	Median	Mode	Minimum	Maximum	
<b>Security Awareness Training (SAT)</b>						
APD	9.0	9.1	9.0	3.0	15	High
APSE	9.1	9.0	9.0	3.0	15	High
ATM	3.5	5.0	5.0	2.0	10	Low
AIR	5.5	6.1	6.0	2.0	10	High

The study findings revealed that security awareness training, in general, have a high influence on the security of electronic health records in the hospital. This is evident from the overall composite score mean of Security Awareness Training (SAT), which stands at approximately 50. It should be noted that this mean falls within the established high security controls range for SAT for this particular study, which spans from 28 to 50 as detailed in Table 3.5.



### 4.3.2 Descriptive Statistics for Security Controls Assessment

The descriptive analysis on security controls assessment revealed that all composite score variables associated with security controls assessment exhibits a normal distribution because the measure of central tendency values are similar as detailed in Table 4.3. The composite score which are all scale variables were classified based on the composite scores interpretation matrix devised in Table 3.5.

**Table 4.3** Key descriptive statistics for Security Controls Assessment

Variable	Measure of central tendency					Security classification
	Mean	Median	Mode	Minimum	Maximum	
<b>Security Controls Assessment (SCA)</b>						
VA	7.5	7.0	8.0	2.0	10	High
LR	10.0	10.0	9.0	3.0	15	High
NR	12.0	10.5	9.0	4.0	20	High
PT	7.5	7.5	7.5	2.0	10	High

The study findings revealed that security controls assessment had high influence on the security of electronic health records in the hospital. This is evident from the overall composite score mean of security controls assessment (SCA), which stands at approximately 55. It should be noted that this mean falls within the established high security controls range for SCA for this particular study, which spans from 25 to 55 as described in detail in Table 3.5.

### 4.3.3 Descriptive Statistics for Security Automation

The descriptive analysis on security automation indicated that all composite score variables associated with security automation exhibits a normal distribution (See Appendix ii, Figure 4.8). The composite score which are all scale variables were classified based on the composite scores interpretation matrix devised in Table 3.5.

**Table 4.4 Key Descriptive Statistics for Security Automation**

Variable	Measure of central tendency					Security classification
	Mean	Median	Mode	Minimum	Maximum	
<b>Security Automation (SAT)</b>						
AM	10.0	10.1	9.0	4.0	20	High
RTD	9.3	9.0	9.0	3.0	15	High
ATT	12.0	12.5	13.0	2.0	10	High

The descriptive statistics results in Table 4.4 has revealed that security automation had high influence on the security of electronic health records in the hospital. This is evident from the overall composite score mean of security automation (SAT), which stands at approximately 45 scores. This demonstrate that this mean falls within the established high security controls range for SCA for this particular study, which spans from 21 to 45 as described in detail in Table 3.5 under the study methodology.

#### 4.3.4 Descriptive Statistics for Behavioral Monitoring

The descriptive analysis results exhibited that all composite score variables associated with behavioural monitoring demonstrated a normal distribution as detailed in Table 4.5. The composite score which are all scale variables were classified based on the composite scores high security and low security as interpretation matrix devised in Table 3.5.

**Table 4.5 Key Descriptive Statistics for Behavioural Monitoring**

Variable	Measure of central tendency					Security classification
	Mean	Median	Mode	Minimum	Maximum	
<b>Behavioural Monitoring (BM)</b>						
CC	15.5	15.0	14.0	2.0	10	High
SC	14.0	14.0	14.0	2.0	10	High
RC	4.3	5.0	5.0	2.0	10	Low
SL	8.5	8.0	8.5	2.0	10	High

The study findings revealed that behavioural monitoring had high influence on the security of electronic health records in the hospital. This is evident from the overall composite score mean of behavioural monitoring (BM), which stands at approximately 40. This imply that the mean falls within the established high security controls range for BM for this particular study, which spans from 21 to 40 as described in detail in Table 3.5.

#### 4.4 Correlations Analysis

To establish the nature and magnitude of correlation among dependent and independent variables of this study, correlation analysis was performed. To ascertain the strength and direction of the association between the dependent and independent variables in this study, Pearson's correlation coefficient was used. It is necessary for the correlation coefficient ( $r$ ) value to fall between -1 and +1. The 1.0 indicates a perfectly positive relationship, 0.5 to 1.0 indicates a stronger positive relationship, 0.5 to 0.1 indicates a weaker positive relationship, 0.1 to 0.1 indicates a little to no relationship, and -1.0 indicates a perfectly negative relationship (Collis & Roger, 2013; Neuman, 2006; Sekeran, 2008; Kothari, 2012).

The correlation coefficients of the five variables: security controls of EHRs, security awareness, security control assessment, security automation and behavioural monitoring are presented in Table 4.6. The findings disclosed that correlation between security awareness and security of EHRs was stronger positive relationship,  $r = 0.631$ ,  $P < 0.01$ . The correlation between security control assessment and security of EHRs was weak positive relationship,  $r = 0.479$ ,  $P < 0.01$ . The correlation between security automation and security of EHRs was stronger positive relationship,  $r = 0.509$ ,  $P < 0.01$  and the correlation between behavioural monitoring and security of EHRs was weak positive relationship,  $r = 0.491$ ,  $P < 0.01$

**Table 4.6 Correlation Analysis for Security Monitoring Practices on EHRs**

<b>Variables</b>		<b>Security awareness</b>	<b>Security assessment</b>	<b>Security automation</b>	<b>Behavioural monitoring</b>	<b>Security of EHRs</b>
Security awareness	Pearson Correlation	1				
	Sig.					
Security assessment	Pearson Correlation	.463	1			
	Sig.	.000				
Security automation	Pearson Correlation	.174	.147	1		
	Sig.	.002	.011			
Behavioural monitoring	Pearson Correlation	.451	.553	.337	1	
	Sig.	.000	.000	.000		
Security of EHRs	Pearson Correlation	.631	.479	.509	.491	1
	Sig.	.000	.000	.000	.000	

\*Correlation is significant at the 0.01 level (2-tailed).

#### **4.5 Multiple Linear Regression Testing**

This section focuses on the findings performed to test the study hypotheses H1, H<sub>2</sub>, H3 to H<sub>4</sub>, aligned with research objectives 1, 2, 3 to 4. The multiple linear regression model adopted to estimate the influence of security monitoring practices on security of electronic health records in Tanzanian public hospitals. The detail of each model are described in subsequent sections.

##### **4.5.1 Influence of Security Awareness Training on Security of EHRs**

This section addresses the first null hypothesis of the study, which stated that security awareness training has no influence on security of electronic health records in Tanzanian public hospitals, in line with objective 1. The influence of security awareness training variables was analysed using a MLR model in two steps. Firstly, the analysis involved utilising composite scores of the SAT constructs (APD, APSE, ATM and AIR) based on the structural model equation (2). Additionally, further

analysis was conducted by examining the individual exogenous indicators within each of the SAT constructs. The regression results for aggregated SAT indicators are given in Table 4.7.

**Table 4.7 Regression results for aggregated SAT indicators**

Model	Unstandardized Coefficients	Standardized Coefficients	t	P-value.
	B	Std. Error	.011 Beta	.171
1 (Constant)	.072	.413		
Awareness on policies and its development	.347	.004	.376	8.472 .000
Awareness on phishing and social engineering	.105	.081	.219	2.397 .000
Awareness on technical measures	.437	.052	.074	9.451 -.006
Awareness on incident responses	.261	.157	.067	1.076 .000

a. Predictors: (Constant), awareness on policies and its development, awareness on phishing and social engineering, awareness on technical measures, awareness on incident responses  
b. Dependent Variable: Security of EHRs

These findings reveal that security awareness training (SAT) has a positive influence on security of electronic health records in Tanzanian public hospitals. Similar to theoretical expectations, all variables i.e. awareness on policies and its development (APD), awareness on phishing and social engineering (APSE), awareness on technical measures (ATM) and awareness on incident responses (AIR) exhibit a positive influence on security of electronic health records statistically significant at  $P=0.05$

#### 4.5.2 Influence of Security Controls Assessment on Security of EHRs

This section addresses the first null hypothesis of the study, which stated that security controls assessment has no influence on security of electronic health records in Tanzanian public hospitals, in line with objective 2. The influence of security controls assessment variables was analysed using a MLR model in two steps. Firstly, the analysis involved utilising composite scores of the SCA constructs (VA, LR, NR and PT) based on the structural model equation (3). Additionally, further analysis was conducted by examining the individual exogenous indicators within each of the SCA constructs. The regression results for aggregated SCA indicators are given in Table 4.8.

**Table 4. 8 Regression results for aggregated SCA indicators**

Model		Unstandardized		Standardized	t	P-value.
		Coefficients		Coefficients		
		B	Std. Error	Beta		
1	(Constant)	.076	1.631		.017	.583
	Vulnerability assessment	.084	.025	.455	8.327	.000
	Log review	.205	.053	.181	2.648	.000
	Network review	.123	.004	.073	4.263	.005
	Penetration test	.016	.103	.029	3.101	.002

a. Predictors: (Constant), vulnerability assessment, log review, network review, penetration test

b. Dependent Variable: Security of EHRs

These findings reveal that security awareness training (SCA) has a positive relationship with security of electronic health records in Tanzanian public hospitals. Similar to theoretical expectations, all variables i.e. vulnerability assessment (VA), log review (LR), network review (NR) and penetration test (PT) exhibit a positive influence on security of electronic health records statistically significant at  $P=0.05$

### 4.5.3 Influence of Security Automation on Security of EHRs

This section addresses the third null hypothesis of the study, which stated that security automation has no influence on security of electronic health records in Tanzanian public hospitals, in line with objective 3. The influence of security automation variables was analysed using a MLR model in two steps. Firstly, the analysis involved utilising composite scores of the SAUT constructs (AM, RTD and ATT) based on the structural model equation (4). Additionally, further analysis was conducted by examining the individual exogenous indicators within each of the SAT constructs. The regression results for aggregated SAT indicators are given in Table 4.9.

**Table 4.9 Regression results for aggregated SAUT indicators**

Model	Unstandardized Coefficients		Standardized Coefficients	t	P-value.
	B	Std. Error	Beta		
1 (Constant)	.109	1.406		.082	.702
Automated measurement	.183	.026	.325	7.349	.000
Reporting tools and dashboards	.084	.223	.134	2.198	.000
Alerting and tracking tools	.135	.281	.096	2.413	.005

a. Predictors: (Constant), automated measurement, reporting tools and dashboards, alerting and tracking tools  
b. Dependent Variable: Security of EHRs

These findings reveal that security automation (SAUT) has a positive relationship with security of electronic health records in Tanzanian public hospitals. Similar to theoretical expectations, all variables i.e. automated measurement (AM), reporting



tools and dashboards (RTD), alerting and tracking tools (ATT) exhibit a positive influence on security of electronic health records statistically significant at  $P=0.05$

#### 4.5.4 Influence of Behavioural Monitoring on Security of EHRs

This section addresses the fourth null hypothesis of the study, which stated that behavioural monitoring has no influence on security of electronic health records in Tanzanian public hospitals, in line with objective 4. The influence of behavioural monitoring variables was analysed using a MLR model in two steps. Firstly, the analysis involved utilising composite scores of the MB constructs (CC, SC, RC and SL) based on the structural model equation (5). Additionally, further analysis was conducted by examining the individual exogenous indicators within each of the SAT constructs. The regression results for aggregated SAT indicators are given in Table 4.10.

**Table 4.10 Regression results for aggregated BM indicators**

Model	Unstandardized		Standardized	t	P-value.
	Coefficients				
	B	Std. Error	Beta		
1 (Constant)	.025	2.179		.074	.762
Counterconditioning	.137	.271	.276	1.179	.000
Stimulus controls	.205	.053	.181	3.894	.000
Reinforcement	.546	.274	.384	5.474	.004
Self-liberation	-.015	.027	.056	9.754	.007

c. Predictors: (Constant), security awareness, security assessment, security automation, behavioural monitoring

Dependent Variable: Security of EHRs

These findings reveal that behavioural monitoring (BM) has a positive relationship with security of electronic health records in Tanzanian public hospitals. Similar to

theoretical expectations, all variables i.e. counterconditioning (CC), stimulus controls (SC), reinforcement (RC) and self-liberation (SL) exhibit a positive influence on security of electronic health records statistically significant at  $P=0.05$

#### 4.5.5 The Overall Regression Analysis

The coefficient of determination explains the percentage of variation in the dependent variable (in this case, the security of EHRs) that can be accounted for by changes in each of the found independent variables (security awareness, security control assessment, security automation and behavioural monitoring. According to the  $R^2$  result, the four independent variables that were investigated can only account for 59.7% of the influence of the independent variables to the security of EHRs. This indicates that additional variables that were not investigated for this study account for 40.3% of the influence of the independent variables on the security of EHRs as indicated in table 4.11.

**Table 4. 11 Model Summary**

Model	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Change Statistics	
								Sig.	F Change
1	.772 <sup>a</sup>	.597	6.31328	.597	109.130	4	295		.000

a. Predictors: (Constant), security awareness, security assessment, security automation, behavioural monitoring

b. Dependent Variable: Security of EHRs

Findings in ANOVA Table 4.12 mentioned that coefficient of determination was statistically significant as evidenced by F ratio ( $n = 109.130$ ) with p value ( $n = 0.000$ )

< 0.05 (Level of significance). The model was therefore able to predict the influence of the security monitoring on the security of the electronic health record (EHR) using security awareness training, security controls assessment, security automation and behavioural monitoring.

**Table 4.12 ANOVA**

<b>Model</b>	<b>Sum of Squares</b>	<b>Df</b>	<b>Mean Square</b>	<b>F</b>	<b>Sig.</b>
Regression	17398.630	4	4349.658	109.130	.000 <sup>b</sup>
Residual	11757.957	295	39.857		
Total	29156.587	299			

a. Dependent Variable: Security of EHRs

c. Predictors: (Constant), security awareness, security assessment, security automation, behavioural monitoring

The results shown that holding the independent variables (Security awareness training, security control assessment, security automation and behavioural monitoring) at constant security of EHRs would be 0.025. Findings showed that the level of security in EHRs increased by 0.647 for every unit increase in security awareness training and by 0.205 for every unit increase in security assessment. Furthermore, the security of EHRs increases by 0.547 when security automation is enhanced by one unit, and by 0.135 when behavioral monitoring is increased by one unit.

**Table 4.13 Coefficients of Regression in Overall Model**

Model		Unstandardized		Standardized	T	P-value.
		B	Std. Error	Beta		
1	(Constant)	.025	2.179		.011	.991
	Security awareness	.647	.061	.455	10.519	.000
	Security assessment	.205	.053	.181	3.894	.000
	Security automation	.547	.056	.384	9.762	.000
	Behavioural monitoring	.135	.117	.056	1.154	.009

a. Dependent Variable: Security of EHRs

b. Predictors: (Constant), security awareness, security assessment, security automation, behavioural monitoring

The first hypothesis of this stated that security awareness has no influence on security of electronic health records in Tanzanian public hospitals. Results in Table 4.6 revealed that security awareness had coefficients of the estimate which was significant based on  $\beta_1 = 0.455$ ,  $p\text{-value} = 0.001$  thus, the null hypothesis was rejected and concluded that there is a significant relationship between security awareness training and security of electronic health records in Tanzanian public hospitals.

The second hypothesis of this study stated that security controls assessment has no influence on security of electronic health records in Tanzanian public hospitals. Nonetheless, the study findings showed that security controls assessment had a positive significant influence on security of EHRs in Tanzanian public hospitals based on  $\beta_2 = 0.181$ ,  $p\text{-value} = 0.000$

The third hypothesis of this study stated that security automation has no influence on security of electronic health records in Tanzanian public hospitals. The study findings showed that security automation had coefficients of estimate which was positive and significant based on  $\beta_3 = 0.384$ ,  $p\text{-value} = 0.000$ .

The fourth hypothesis of this study stated that behavioural monitoring had no influence on security of electronic health records in Tanzanian public hospitals. Based on the findings the null hypothesis was rejected based on  $\beta_4 = 0.056$ , p-value = 0.009. This suggests that there is up to 0.056 unit increase in security of EHRs for each unit increase in behavioural monitoring on security of electronic health records.

## **CHAPTER FIVE**

### **DISCUSSION OF FINDINGS**

#### **5.1 Chapter Overview**

This chapter discusses the results as presented in chapter four of this study. It provides interpretations and meanings of the results in relation to the research problem's objectives implied in chapter one and in chapter two of this study. The results discussed in this chapter are obtained as the application of the methods implied in chapter three. The results discussed led to the summary, conclusions and implications of the study as addressed in chapter six.

#### **5.2 Demographic Profile of Respondents**

This part offers a briefly discussion on the demographic description of this Study. Demographic information refers to the personal characteristics such as gender, age, occupation, years of working experience, working places and education level. The table 4.1 in chapter 4 showed the demographic information results. The study included 300 respondents currently working in public hospitals in Tanzania. The participants were requested to provide demographic information in relation to their gender, age, education level, working experience and the hospital they work in. The results from questionnaire on gender indicated the proportionality of males and female's participants in this study, hence gender balance.

Furthermore, findings specified that the majority of participants were in the age group between 20-30, 31-40 and 41-50 which implies that all were matured enough to provide constructive ideas on the topic under study. Furthermore, the results indicated that the majority had bachelor degree and diploma as their highest

education level hence, they were educated enough to provide their opinions on the study subject. Furthermore, results indicated that majority of respondents had spent more than 5 years working at the hospitals, which means that they were more knowledgeable about the security monitoring and security controls of EHRs. Moreover, the results indicated that the participants were comprised of IT officers, medical doctors, nurses, pharmacists, health laboratory technologists, record officers and administrative officers. This implies that all of the respondents were the key users of EHRs hence, were appropriate to this study.

### **5.3 Influence of Security Awareness Training on Security of EHRs**

The results showed that security awareness training had a positive influence on security of electronic health records in Tanzanian public hospitals. The positive influence implies that as the hospitals invest on security awareness training to its employee the more patient's information kept in health information systems are secured. Furthermore, the analysis from multiple linear regression model indicated a significant and positive influence of security awareness to security of EHRs in the hospital, (Beta= 0.647,  $t_1= 10.519$ , sig. = p-value =  $0.000 < 0.05$ ). This indicates the strong level of association between security awareness training and security of EHRs in the hospitals. This results were relatively similar to the findings from other scholars who argued that if training and awareness elements are ignored in security controls of electronic health records the effective security controls will never be achieved (Abuhammad et al. 2020; Zamir 2020; Ban Issa et al., 2020; Nisreen, 2018). This result was also in line with the theories which guided this study

Contrarily, even though security awareness training exhibited a positive influence on security of electronic health records in the public hospitals, individual indicators within this construct reveal different influences. For instance, ISA3 (awareness on technical measures) have adverse influence on security of electronic health records. This finding is aligned with other previous research which indicated that awareness on technical measure is weak associated with security of electronic health records since users of EHRs is just required to have a few basics of security controls and not technical skills (Asogwa 2012; Cucoran et al., 2013). The negative influence of ISA3 (awareness on technical measures) implies that even if users are not well trained on technical measures the security of electronic health records will be achieved.

Conversely, ISA1 (awareness on security policies and its development) and ISA4 (awareness on incident response), had a positive and strong influence on the security of electronic health records in Tanzanian public hospitals. The positive influence of ISA1 and ISA4 on the security of electronic health records is in line with other scholars who argue that awareness on appropriate security policies and incident responses strongly influence security controls in healthcare organizations (Conaty (2017; Peikari, Ramayah, Shah & Lo 2018). This finding possibly suggest that the awareness on security policies (ISA1) and the awareness on incident responses (ISA4) may be perceived to influence other aspects of security controls such as technical controls and phishing and social engineering in electronic health records. Consequently, healthcare organizations are more likely to be secured when users are aware on security policies and incidence responses.



On the other hand, findings revealed that ISA2 (awareness on phishing and social engineering) had a positive influence on security of electronic health records in the public hospitals. This finding aligns with the research conducted by Conaty (2017), who found that healthcare industry is targeted greatly by phishing and social engineering attacks hence, make the knowledge and education regarding phishing and fraud emails essential so that they will understand how to detect and keep away from the phishing attacks. This means that higher levels of awareness on phishing and social engineering is likely to enhance users' confidence leading to more security controls in electronic health records in the hospitals.

#### **5.4 Influence of Security Controls Assessment on Security Controls of EHRs**

The study findings showed that the security controls assessment had a positive influence on security of electronic health records in Tanzanian public hospitals. These findings suggest that when public hospitals conduct security controls assessment of its health information systems increases the chance to secure electronic health records since through security controls assessment the system administrators are able to identify the existing weakness in the information systems. These findings are in consistent with the results by (Ayatollahi & Shagerdi 2017; Conaty-Buck 2017) who found that security controls assessment help hospitals to identify irregularities and parties of the systems which is underperforming. Once the system administrators identify the loophole through security assessment in the systems it become easily to come up with remedial measures.

Specifically, the results showed that the vulnerability assessment (SCA1) had a positive influence on security of electronic health records in Tanzanian public

hospitals. These results imply that the more public hospitals conduct security controls assessment through vulnerability assessment the chances for increasing security of electronic health records increases. According to Conaty-Buck (2017) risk and vulnerability assessments help the hospitals to identify the existing weakness in the information system or in the new hardware or software installed which can be used by the attackers. This may also possibly suggest that regular vulnerability assessment obvious protect electronic health records into attackers. Thus, the lack of vulnerability assessment is likely to act as catalysts to the security and privacy breaches of patient's information.

On the other hand, findings revealed that log review (SCA2) and network review (SCA3) had a positive influence on security of EHRs in the public hospitals. This imply that the public hospitals should conducted an audit log and network review, which is extremely important information on who uses the hospital system, what medical data is accessed, what entries were created or altered, by whom, and when. This helps the hospitals to monitor the system access and the activities performed by those who accessed the EHR systems. This finding aligns with HIPAA (2015) which stated that the review of audit trail logs helps to identify and monitor all access to the systems and removal unnecessary access rights. Similarly, Capelão and Barbosa (2018) drew attention to the need for regular review of the systems to check how well it has been configured. Thus, lack of regular system configuration results in privacy and security breaches of patient information, as mentioned by Shamsi and Khojaye (2018), who agreed with Capelão and Barbosa that misconfigured

information systems and poor network review are the leading causes of loss of confidentiality in an information system.

Moreover, SCA4 (penetration test) exhibit a positive influence on security of electronic health records in Tanzanian public hospitals. The positive relationship between penetration test and security of electronic health record indicates that the more public hospitals conduct penetration test to its health information systems the more electronic health records become secured. This finding is in line with theoretical expectation and results from other previous researches, indicating that penetration test positively influence security of electronic health records in Tanzanian public hospitals (Ayatollahi & Shagerdi 2017; Conaty-Buck 2017). This finding imply that increased penetration test may increases the chance to detect all parts of the systems which are not working proper and hence increases the chances for improvement.

### **5.5 Influence of Security Automation on Security of EHRs**

The findings showed that security automation had a positive influence on security of electronic health records in Tanzanian public hospitals. These results imply that the more public hospital increases the automation of its security systems the more electronic health records become secured. These findings aligned with the theoretical expectation and other previous studies on the same topic, which indicate that the more security systems are automated the higher the security controls (Capelão 2018; Collier, Ives, & Bey 2013). Similarly, Collier (2014) and Ives (2014) indicated a positive relationship between security automation and security controls of EHRs on 26.5 percent of the variability was explained suggesting that other factors are also

important for security controls of EHRs. On other hand, AbiolaIdowu and Adedokun, Taiwo Oyewole (2013), in their study on the effects of monitoring and control activities on fraud detection found that computerization in the form of automation had T- value of 3.128 and a P-value of 0.004\*\* (2-asterisks) means security automation had a positive significant relationship on fraud detection in the selected banks.

Conversely, SAT1 (automated measurement) had a negative influence on security of electronic health records in the public hospitals. The negative influence of SAT1 on security of electronic health records is in line with other scholars who argue that automated measurement is weak in supporting security of electronic health records (Bey & Magalhaes 2013; Capelo & Barbosa 2018). This unexpected negative outcome contrary of direct relationship between automated measurement in security of electronic health records suggests that even in absence of automated measurement security of electronic health records can still be achieved. This may also possibly suggest that the reporting tools (SAT2) and alerting and tracking tools (SAT3) may be considered positively influencing security of electronic health records in the hospitals. Contrarily, AlSadhan, (2016) argued that public hospital needs to invest heavily in security automation because automation enables the collection and consolidation of data, correlation, and decision-making in ways that human cybersecurity professionals cannot. For instance, automating the updating of virus signatures will not protect against a heretofore unseen virus.

On the other hand, both SAT2 (reporting tools and dashboards) and SAT3 (alerting tracking tools) exhibited a positive relationship with security of electronic health

records in Tanzanian public hospitals. This finding aligns with the conclusion of Collier (2014) which found that the use of reporting tools and tracking tools enhance the fast responses to the adverse situations in healthcare information systems hence increases security controls in electronic health records systems. The implications of this finding is that when systems are set with automatic reporting tools and tracking systems give system administrator a chance to be well informed on any kind of threats and risks to the health information systems. These tools act as a watch dog which increases the confidence to system administrators and hospital's management as it provides instant feedback of what is happening in the systems.

#### **5.6 Influence of Behavioural Monitoring on the Security of EHRs**

The study result indicated that the behavioural monitoring had a positive influence on security of electronic health records in Tanzanian public hospitals, although this effect is not statistically significant at a significance level of  $P=0.05$ . These findings imply that the more public hospitals monitor its users' behaviours increases the chances to secure patient's information. The finding was in line with Abiola, Idowu and Adedokun, TaiwoOyewole (2013) who stated that when users are aware that their work and practices may be witnessed by others, particularly in the event of non-compliance or misconduct at work (i.e., non-compliance with information security policy requirements) will do their utmost to act according to the required practices. The result by Vucetic et al. (2011) stated that users should be enforced to comply with security controls by penalizing/ punishing users of information systems on misbehaviours in information system or security controls, this can increase security compliance behaviours. With specific rewards and losses, security controls can be

enforced more effectively. For example, healthcare organization should enforce fines (kind of punishment learning) to all users/employees who do not comply to information security policies.

Similarly, even though behavioural monitoring exhibit a positive influence on security of EHRs, individual indicators within this construct reveal different effects. For instance, BM1 (counterconditioning) and stimulus control (BM2) had an adverse influence on security of electronic health records in public hospitals. This finding is aligned with other previous research which indicated that users' stimulus substitution may minimize the confidence of users in information systems hence, results into adverse conditions in electronic health record systems (Kamoun & Nicho 2014; Hassidim et al., 2017). This is in consistent with the findings by Andriole (2014), who stated that stimulus controls such as implementation of disciplinary actions for the repetitive disobedience of security controls should be implemented to encourage all users to adhere with the hospitals' security policies and procedures. This may imply that by associating beneficial behaviors with the stimuli, undesirable behaviors or responses to it can be trained into desired behaviors or responses.

On the other hand, findings revealed that reinforcement (BM3) had a positive influence on security of electronic health records in the hospitals. This means that that users are demanded to adhere with the better security practices when interacting with health information systems in the hospital. This results are in consistent with the findings by (Andriole 2014), who stated that disciplinary actions for the repetitive disobedience of security policies and procedures should be implemented to encourage all users to adhere with the hospitals' security policies and procedures.

Similarly, the results of (Vucetic et al., 2011) assert that healthcare organizations are required to reinforce some of user's behaviour by conducting strict review of user's access right at regular intervals. This means that all users' access right should be granted for certain period, and its review should be conducted at a regular interval to ensure effective behavioural monitoring.

Moreover, BM4 (self-liberation), had a positive influence on security of electronic health records in the hospitals. This means that users willingly should develop the compliance behaviour when interacting of health information systems. This finding aligns with the research conducted by Maqbool et al. (2020), which found that when users are well trained what is expected is their adherence to the stated security policies and procedures, if users fail to adhere to policies, punishments should be imposed according to the stated disciplinary actions. Similarly, the study conducted by Eskritt et al. (2014) added that when users are well trained they get to think about the future consequences of their behaviours.

The general findings revealed that all four factors were realised to be significant and predictors of security of electronic health records in Tanzanian public hospitals. The independent constructs explained 59.7% ( $R^2=0.597$ ) of the variance in security of EHRs. This indicates that the model provides a strong level of predictive accuracy for security controls of EHRs. Of these factors, information security awareness training and security automation turned out to be the strongest predictors with a large effect size in influencing security controls of EHRs in contrast security assessment and behavioural monitoring which had a medium effect size. These findings are logical since hospitals may better communicate their information security policies,

strategies and procedures to their staff with the use of information security awareness. This will increase employee adherence to EHR security controls. The capacity to elicit compliance determines how strong the effect is. On the other hand, security automation plays a big role in ensuring security controls are effective without even the need for human interactions.

Similarly, Alqahtani and Braun (2021) supported this finding in their study on, *Examining the Effect of Technical Control, Accountability and Monitoring on Cyber Security Compliance in e-Government Organizations*, which found that monitoring and control, or information security monitoring and evaluation, is a strong predictor of cyber security compliance. In the regression equation, monitoring and control was found significant with  $R^2=.007$ ,  $F(1, 296) = .33$ ,  $p < 0.01$ . Monitoring of information systems is directly related to accountability because, without strong monitoring and evaluation mechanisms, accountability cannot be enforced. If an individual's perception of accountability is strong and observed by the individual, then the compliance behaviour on security controls will be strong.

Likewise, Abiola, Idowu and Adedokun, TaiwoOyewole (2013), in their study on the effects of monitoring and control activities on fraud detection, supported this study's finding as they found that monitoring activities had a positively significant at 5% level, adjusted  $R^2$  was 0.542, which implied that 54.2% of the variation on performance was explained by monitoring activities in the model. When an organization carry out appropriate security monitoring practices in its information systems all part of information systems become secured.



The study carried out by Balozian (2017) to identify factors affecting employee's compliance behaviour to security controls, was in the same line with this study's finding as he revealed that monitoring and control are among the factors that influence the behaviour of the employee in terms of compliance with security controls. Despite the differences in context and geographic location where the cited research has been conducted, the results are consistent and valid to support findings of this study as it intended to assess the influence of behavioural controls.

For instance, users' who are familiarity with monitoring practices they understand that their work and practices may be witnessed by others, particularly in the event of non-compliance or misconduct at work (i.e., non-compliance with information security policy requirements) and will do their utmost to comply with the policy. Monitoring and evaluation can be leveraged in the context of information security compliance as an efficient way to promote and facilitate security compliance and to automate security controls for healthcare organizations. When information security monitoring is integrated into the normal IT and security management processes, monitoring is efficient and makes insiders expect to be monitored for their activities toward security compliance. In addition, monitoring, evaluating and performing systems audits/ assessment are effective ways to comply with data protection laws.

The findings of this study implies that public hospitals need to consider investing more on M&E particularly security monitoring practices by increasing information security awareness training programs for their employees, implementing regular security control assessments, increasing the level of training and training should be participatory and focus on all important aspects of information security controls.

Further, the hospitals are required to put more effort into security assessment, security automation and behavioural monitoring because security controls of EHRs increase with the increase in both of the four monitoring activities, i.e., information security awareness training, security assessment controls, security automations and behavioural monitoring.

## CHAPTER SIX

### CONCLUSION AND RECOMMENDATIONS

#### 6.1 Chapter Overview

The chapter presents the summary, conclusions, recommendations and implications for the study. It concludes the findings of study by summarizing the principal findings and pertinent conclusions of the study. It further gives recommendations and areas for future research and implications for the study findings. The summary, conclusions, recommendations and implications addressed in this chapter are originally drawn from chapter one, two, three, four and five.

#### 6.2 Conclusions

The first objective of this study intended to examine the influence of security awareness training on the security of EHRs in Tanzanian public hospitals. The results discovered that security awareness training had a positive significant influence on security of electronic health records, (Beta= 0.647,  $t_1= 10.519$ , sig. = p-value =  $0.000 < 0.05$ ). Based on the evidence from this study's findings the conclusions can be drawn as follows. First, the study has shown that conducting information security awareness training led to the realization of security controls of electronic health records in public hospitals. Second, the results of the study have demonstrated a strong and positive relationship between security awareness training and security controls in electronic health records in a Tanzanian public hospital. Hence, the study reaches the conclusion to reject the null hypothesis and accept the alternative hypothesis.

The second objective of this study examined the influence of security controls assessment on the security of EHRs in Tanzanian public hospitals. The results revealed that security controls assessment had a significant positive effect on security of EHRs in public hospitals, (Beta= 0.205,  $t_2 = 3.394$ , sig. = p-value =  $0.000 < 0.05$ ). Based on the study's findings and discussion in chapter five, it is concluded that security controls assessment has a moderate and significant effect on security of electronic health records in a Tanzanian public hospital. Therefore, the null hypothesis which stated that "security controls assessment has no influence on security of electronic health records in Tanzanian public hospitals" was rejected.

The third objective of this study examined the influence of security automation on the security of EHRs in Tanzanian public hospitals. The result shows security automation positively influence security of electronic health records (Beta= 0.547,  $t_3 = 9.762$ , sig. = p-value =  $0.000 < 0.05$ , The findings show a statistically significant, a moderate and positive influence among security automation and the security of electronic health records in Tanzanian public hospitals. Hence, it is concluded that the security automation has a significant influence on the security controls of electronic health records in Tanzanian public hospitals. Thus, the null hypothesis which stated that security automation has no influence on the security of electronic health records in Tanzanian public hospitals was rejected.

The fourth objective of this study examined the influence of behavioural monitoring on the security of EHRs in Tanzanian public hospitals. The results revealed a statistically significant, a moderate and positive effect between behavioural monitoring on security of electronic health records in Tanzanian public hospitals

(Beta= 0.135,  $t_4= 1.154$ , sig. = p-value = 0.049<0.05). Therefore, the study concludes that behavioural monitoring had a significant influence on the security of electronic health records in Tanzanian public hospitals. Therefore, the hypothesis which stated that behavioural monitoring has no influence on the security of electronic health records in Tanzanian public hospitals was rejected.

Generally, the findings indicated that all four variables were found to be a significant and positive predictors of security in EHRs. The independent variables explained 59.7% ( $R^2=0.597$ ) of the variance in security of EHRs. The study concludes that security monitoring practices had a significant positive influence on the security of electronic health records in Tanzanian public hospitals. Thus, public hospitals investment in both security awareness training, security controls assessment, security automation and behavioural monitoring for effective security of electronic health records. Thus, all the four hypotheses in this study were rejected.

### **6.3 Recommendations**

Based on the study findings, the study recommends the adoption of security monitoring practices in electronic health records in Tanzanian public hospitals. This should involve capacity-building initiatives to the users of EHRs systems, establishment of strong security controls assessment, improvement of security infrastructure to allow for security automation and the use of users behavioural monitoring. The specific recommendations on practices, theory and policy are summarized in the following subsections.

### **6.3.1 Practical Recommendation**

Based on the study findings and conclusions, the study recommends that public hospitals should practicing continuous security monitoring to its electronic health systems. In conducting security monitoring more emphasises should be on conducting regular security awareness and training to all staff involved in the health information systems. The users of the system should have necessary knowledge such as awareness on security policies and standards, awareness on phishing and social engineering, awareness on technical measures and awareness on incident responses.

Furthermore, the study recommended that public hospitals should practice regular security controls assessment to its health information systems in order to assess its performance. Based on the study findings the security controls assessment should focus on vulnerability assessment, log review, network review and penetration tests. This is also in line with assumptions of the theories which used to guide the study. The well trained system administrators should be used to conduct security controls assessments and all findings should be documented and discussed in the hospital's management meetings for immediately solutions to the emerging problems.

Furthermore, based on the result of the study, it is recommended that the public hospitals should implement effective security automation mechanisms in its information systems. This will not only contribute protection of the hospital's network from attackers but also will allow systems administrators to engage in other productive works in their department. The study also recommends the combination of automation tools as these tools have different capabilities, for example, intrusion

prevention system (IPS) can spot and recognize attacks that a firewall and antivirus cannot detect for example, double denial of service attacks.

Moreover, it is recommended that public hospitals should perform behaviour monitoring practices to its users of electronic health records as users of the systems since users have a greater influence on security controls. The behavioural monitoring is recommended to focus on the stimulus controls by making users willing to comply with security controls, reinforcement by the use of appropriate disciplinary actions, counterconditioning by controlling all users' actions to comply with security controls and self-liberation with the use of security awareness campaigns.

### **6.3.2 Theoretical Recommendations**

As predicted by both theories, quantitative evidence generated by this thesis support the theoretical proposition that security monitoring practices has beneficial influence in security of electronic health records in Tanzanian public hospitals. In order to increase the applicability of the theory of planned behaviour in the study of security monitoring practices, the study recommends the other variables which influence behavioural intention and motivation such as stimulus controls and past experiences be included in the theory of planned behaviour as its influence has been justified from the findings of this study.

By incorporating aspects such as stimulus controls and past experiences in the theory of planned behaviour will broaden the ground for the theory in its applicability to study of behaviour controls in information security controls and monitoring and other fields.

### **6.3.3 Policy Recommendation**

Based on the study's findings and theories which were used to guide this study it has been demonstrated that security monitoring practices positively influence the security of electronic health records in the public hospitals it is therefore, recommended that a thoroughly policy review be conducted to incorporate the issue of security monitoring practices in the existing national health policy. This is due to the fact that the available eHealth policy in public hospitals is not detailed enough to influence security monitoring practices. Since, most of the national health policy was created before the intensive application of ICT in healthcare service delivery, national health policy particularly eHealth policy should be reviewed to prioritise the security and privacy controls of patient's information.

Moreover, to build a very supportive policy which may address all security issues in electronic health records, a link between policy makers and the key users of health information systems should be created. The key users such as IT officers, medical doctors, nurses, pharmacists, laboratory technologists, records, administrative staff should be the part of review process. This will create an environment to influence acceptance and adherence to the developed policy.

### **6.4 Recommendations for Further Research**

The study limited itself into six public hospitals in Tanzania, its countermeasures and employees' experiences. The future study should be conducted across all spectra of public hospitals to find out the influence of security monitoring practices on the security of electronic health records in Tanzanian public hospitals. Conducting research in many hospitals will provide more accurate conclusions and permit for



more generalizability. Additionally, given this study was conducted to public hospitals only, future research should include both public and private hospitals in Tanzania to get general view on the influence of security monitoring and evaluation practices on security of electronic health records in Tanzanian hospitals.

Future research can be pursued in public hospitals in other regions to elucidate information from different demographic groups which can help to deliver much greater insight in the area and allow for much healthier generalizations. The present study used a cross-sectional research design, thus there is a need for future research to consider a comparative analysis between Tanzania and other African countries to explore their security strategies and practices in monitoring of security of EHRs and to compare the results. The study adopted a quantitative research method. Therefore, future research should consider using other approaches like the qualitative approach only or the mixed method approach. Lastly, this study used multiple linear regressions, the future research can be done using other advanced analysis techniques like structural equation modelling (SEM) which can release direct and indirect relationships simultaneously.

### **6.5 Implications of the Study**

The findings of this study have extensive implications for theory, practices and knowledge in general. The results provide values for Tanzanian public hospitals in connection to the application of security monitoring practices in electronic health records. The specific implications of the study based on, practice and theory as summarized in the following subsections.

### **6.5.1 Implications for Practices**

From a health practice perspective, the findings of this study have significant implications for the government, communities and researchers. First, this study's findings can help to improve practice by providing an in-depth analysis of current situation regarding the influence of security monitoring practices on safeguarding electronic health records at public hospitals. The study contributes to practice by foregrounding the necessity for government through the Ministry of Health and hospital management to put more emphasis to its hospitals to practice effective security monitoring, further, the study workup the IT staff, hospital managers and stakeholders in the hospitals to practicing continuous security monitoring in order to ensure security of EHRs.

Further, the study contributes to practice by identifying some strategies for effective information security monitoring of EHRs in the hospitals. The study provides a new study area that may be investigated by scholars and researchers interested in the field of health information security particularly in developing countries such as Tanzania where the development of electronic health records is still in infancy stage.

### **6.5.2 Theoretical Implications**

In the theoretical review in chapter two of this study, it was argued based on theory of planned behaviour that user's security awareness can result into realization of user's intention to security controls. In addition, it was asserted, using integrated system theory that security assessment, security automation facilitates the security controls in an organization. As predicted by both theories, quantitative evidence generated by this thesis support the theoretical proposition that security monitoring

practices has beneficial influence in security of electronic health records. Thus, the generated evidence supports the applicability of integrated theory and theory of planned behaviour.

Additional to theoretical implications, this study created a conceptual framework that offers a methodological approach comprehending security monitoring practices on EHR security controls. The study suggests that stimulus controls and pas experiences to be included in the theory of planned behaviour as both of this constructs have proved to influence intention to participate in a certain behaviour hence, theoretical contributions

## REFERENCES

- Abiola, I., & Oyewole, A. T. (2013). Internal control system on fraud detection: Nigeria experience. *Journal of Accounting and Finance*, 13(5), 141-152.
- Abuhammad S, Alzoubi KH, Al-Azzam SI, Karasneh RA. (2020). Knowledge and practice of patient's Data Sharing and Confidentiality among Nurses in Jordan. *J Multidiscip Healthc.* 2020 Sep 16;13: 935-942.doi: 10.2147/JMDH.S269511.PMID: 32982270; PMCID: PMC7502382
- Addy D and Bala P (2016). Physical access control based on biometrics and GSM. *International Conference on Advances in Computing, Communications and Informatics.* DOI:10.1109/ICACCI.2016.7732344 Corpus ID: 15967367
- Ademuyiwa, I & Adeniran A (2020). *Assessing Digitization and Data Governance Issues in Africa*, Ontario: CIGI Paper NO. 244
- Ajzen, I. (1985). From intentions to actions: A theory of planned behaviour. *In Action control* (pp.11-39). Springer, Berlin, Heidelberg.
- Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Alhazmi, O. H. (2015). Computer-Aided Disaster Recovery Planning Tools (CADRP). *International Journal of Computer Science & Security (IJCSS)*, 9(3), 132–139
- Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. *Quality progress*, 40(7), 64-65.

- Aljumaili Mustafa (2016). *Data quality assessment: Applied in Maintenance*. DOI: 10.13140/RG. 2.1.3386.6641
- Alqahtani, M., & Braun, R. (2021). *Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organizations*. [https://web.archive.org/web/20210428072623id\\_/https://www.researchsquare.com/article/rs-196216/v1.pdf](https://web.archive.org/web/20210428072623id_/https://www.researchsquare.com/article/rs-196216/v1.pdf)
- Alsadhan, T., & Park, J. S. (2016, June). Security automation for information security continuous monitoring: Research framework. In *2016 IEEE World Congress on Services (SERVICES)* (pp. 130-131). IEEE.
- Altaf, I., Ul Rashid, F., Dar, J. A., & Rafiq, M. (2016). Vulnerability assessment and patching management. In *International Conference on Soft Computing Techniques and Implementations, ICSTI 2015, 8-10 Oct. 2015, Faridabad, India* (pp. 16–21). IEEE.
- Andriole, KP. 2014. Security of electronic medical information and patient privacy: what you need to know. *Journal of the American College of Radiology* 11(12): 1212-1216.
- Argaw Salema, Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burlison, Jan-Michael Vogel, Chana O’Leary, Bruce Eshaya-Chauvin and Antoine Flahault (2020). Cybersecurity of hospitals: *discussing the challenges and working toward mitigating the risk*. <https://doi.org/10.1186/s12911-020-01161-7>

- Asogwa, B. E. (2012). The challenge of managing electronic records in developing countries: Implications for records managers in sub-Saharan Africa. *Records Management Journal*, 22(3), 198-211.
- Ayatollahi, H & Shagerdi, G. (2017). Information security risk assessment in hospitals. *The Open Medical Informatics Journal* 11(3): 37.
- Babbie, E. (2002). *The basics of social research*. Belmont, CA: Wadsworth Publishing
- Baguley, T. (2012). *Serious stats: A guide to advanced statistics for the behavioural sciences*. London : Palgrave Macmillan.
- Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., and van Dijk, B. (2019). Informing, simulating experience, or both: a field experiment on phishing risks. *PLoS One* 14: e0224216. doi: 10.1371/journal.pone.0224216
- Ball, R. A., Lilly, J. R., & Cullen, F. T. (2010). *Criminological theory: Context and consequences*. Thousand Oaks, Sage Publications, Incorporated.
- Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 48(3), 11-43.
- Ban Issa W, AL Akour I, Ibrahim A, Griffiths J. (2020). *Privacy, confidentiality, security and patient safety concerns about electronic health records*. *IntNurs Rev*. 2020 Jun; 67(2):218-230. Doi: 10.1111/inr.12585. Epub 2020 Apr 21. PMID: 32314398.

- Baruah, N. (2013). System Diagnosis and Fault Tolerance for Distributed Computing System: A Review. *International Journal of Computer Science & Communication Networks*, 3(4), 284–295.
- Baset, A. Z., & Denning, T. (2017). IDE Plugins for Detecting Input-Validation Vulnerabilities. *In 2017 IEEE Security and Privacy Workshops (SPW)*, 25–25 May 2020, San Jose, CA, USA (pp. 143–146). IEEE.
- Batchellor, V. (2016). *Get the security budget you need and spend it wisely*. Retrieved Dec 08, 2016, from <https://securityintelligence.com/get-the-security-budget-you-needand-spend-it-wisely/>
- Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behaviour. *Journal of research in personality*, 25(3), 285-301.
- Belle, J.P.V et al., (2018). Africa Data Revolution Report: Status and Emerging Impact of open Data in Africa, Washington: *World wide web foundation*
- Bey, J. M., de Magalhães, J. S., Bojórquez, L., & Lin, K. (2013). Electronic Health Records in an Occupational Health Setting—Part II. Global Deployment. *Workplace Health & Safety*, 61(3), 95-98.
- Bosworth, S., Kabay, M, & Whyne, E. (2014). Computer Security Handbook (6th Editio). *John Wiley & Sons, Inc.*, Hoboken, New Jersey.
- Braithwaite, A., & Li, Q. (2007). Transnational terrorism hot spots: Identification and impact evaluation. *Conflict Management and Peace Science*, 24(4), 281-296.
- Bryman, A. (2012). *Social Research Methods*. 4th edn. Oxford: Oxford University Pres

- Busagala L. S. P. and Kawono G. C. (2013a). Underlying Challenges of E-Health Adoption in Tanzania. *International Journal of Information and Communication Technology Research*. Volume 3No. 1, January. ISSN 2223-4985
- Bowen, Glenn, A., (2009). Document Analysis as a Qualitative Research Method, *Qualitative Research Journal*. DOI: 10.3316/QRJ090202
- Cadick R. (2005). *Protecting networked medical devices from worms and viruses*. Biomedical Instrumental Technology.
- Calic, D., Pattinson, M., and Parsons, K. (2016). “Naive and accidental behaviours that compromise information security: what the experts think,” in *Proceedings of the 10th International Symposium of Human Aspects of Information Security and Assurance*, eds N. L. Clarke and S. M. Furnell (Frankfurt: HAISA).
- Carneiro, I., & Howard, N. (2011). *Introduction to epidemiology*. ed. Maidenhead, Berkshire.
- Castillo, E. (2009). Process optimization: A statistical approach. *Journal of Quality Technology*, 40(2), 117-135.
- COBIT (1996), COBIT: Control Objectives, ISACA, Rolling Meadows, IL. Collier, R. 2014. *New tools to improve safety of Electronic Health Records*. CMAJ 186(4): 251251
- Chen, L., & Chen, L. (2017). *Scholarship at UWindsor Security Management for the Internet of Things* by. The University of Windsor. Retrieved from <https://elk.adalidda.net/2017/08/Security-Management-for-IoT.pdf>



- Chen, Y., Ramamurthy, K. R., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, 55, 11–19. Retrieved from <http://www.iacis.org/jcis/jcis.php>
- Chuma, J.M., G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Sanenga, A., Mapunda. (2020). An overview of key technologies in physical layer security. *Entropy*, 22(11), 1261.
- Cohen, J. (1988). *Statistical power analysis for the behavioural sciences*. 2nd. Hillsdale, NJ: erlbaum.
- Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioural sciences*. Routledge
- Cohen, H. H., & Cleveland, R. J. (2013). Safety program practices in record-holding plants. *Professional Safety*, 28(3), 26-33.
- Cohen, P., West, S. G., & Aiken, L. S. (2014). *Applied Multiple Regression/Correlation Analysis for the Behavioural Sciences*. Psychology Press.
- Collier, R. 2014. *New tools to improve safety of Electronic Health Records*. CMAJ 186(4): 251251
- Collin, M., McGovern, N., & Haniffa, M. (2013). Human dendritic cell subsets. *Immunology*, 140(1), 22-30.
- Conaty-Buck, S. (2017). Cybersecurity and healthcare records. *Am Nurse Today*, 12(9), 62-64.

- Constantine Mircioiu and Jeffrey Atkinson (2017). A Comparison of Parametric and Non-Parametric Methods Applied to a Likert Scale. *Pharmacy* 2017, 5, 26; doi:10.3390/pharmacy5020026
- Cooper, H., Robinson, J. C., & Patall, E. A., (2006). Does homework improve Academic achievement? A synthesis of Research 1987—2003. *Review of Educational Research*, 76(1), 1 - 62.
- Corcoran, R. B., Cheng, K. A., Hata, A. N., Faber, A. C., Ebi, H., Coffee, E. M., ... & Engelman, J. A. (2013). Synthetic lethal interaction of combined BCL-XL and MEK inhibition promotes tumor regressions in KRAS mutant cancer models. *Cancer cell*, 23(1), 121-128.
- Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 4th ed., Sage Publications, California
- Creswell, J.W. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage, Los Angeles
- Crossler, R. E., & Bélanger, F. (2006, September). The effect of computer self-efficacy on security training effectiveness. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 124-129).
- Dalglis, S. L., Khalid, H. & McMahon, S. A. (2020). Document analysis in health policy research: the READ approaches. *Health Policy and Planning*, 35(10), 1424–1431

- David, F. G., Patrick, W. S., Phillip, C. F., & Kent, D. S. (2010). *Business Statistics*. Pearson publishers, New Jersey.
- Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162-176.
- De Winter, J. C., Gosling, S. D., & Potter, J. (2016). Comparing the Pearson and Spearman correlation coefficients across distributions and sample sizes: A tutorial using simulations and empirical data. *Psychological methods*, 21(3), 273.
- Doll, J., & Ajzen, I. (1992). Accessibility and stability of predictors in the theory of planned behaviour. *Journal of personality and social psychology*, 63(5), 754.
- FFIEC (2006). "Information Systems IT Examinations Handbook." 138
- Gao, Xiangzhu et al. "Implementation of E-Health Record Systems and E-Medical Record Systems in China". *The International Technology Management Review* 3.2 (2013): 127-139
- Ifinedo, P. (2014). Information systems security policy compliance: an empirical study of the effects of socialization, influence, and cognition. *Inf. Manag.* 51, 69–79. doi: 10.1016/j.im.2013.10.001
- Ipswitch. (2010). *Best Practices: Event Log Management for security and compliance initiatives*. Retrieved Nov 20, 2016, from [https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/ELM\\_Security\\_WP.pdf?ext=.pdf](https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/ELM_Security_WP.pdf?ext=.pdf)

- Ives, TE. 2014. The new 'e-clinician' guide to compliance. *Audiology Today* 26(1): 52-53. *International Organization of Standardization*. 2008.
- ISO27799:2008: *Health informatics: information security management in health using ISO/IEC 27002*. Available from: <https://www.iso.org/standard/41298.html> (Accessed 21 July 2020).
- ISO/IEC. (2005). ISO/IEC 17799:2005(E) *Information Technology Security Techniques, Code of Practice for Information Security Management*. Geneva, Switzerland: ISO/IEC.
- Fernandez-Aleman JL, Señor, IC. Lozoya, PA &Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics* 46(3): 541-62.
- Elfil, M., & Negida, A. (2017). Sampling methods in clinical research; *an educational review*. *Emergency*, 5(1), 1-5
- Elkamchouchi, H. M. (2018). An Advanced Hybrid Technique for Digital Signature Scheme. In 2018 5th *International Conference on Electrical and Electronic Engineering (ICEEE)*, 3-5 May 2018, Istanbul, Turkey (pp. 375–379). IEEE.
- ESG Research Report (2016). *Network security monitoring trends, 2016 IT Spending Intentions Survey*.
- Eskritt, M., Doucette, J., and Robitaille, L. (2014). *Does future-oriented thinking predict adolescent decision making? J. Genet. Psychol.* 175, 163–179. doi: 10.1080/00221325.2013.875886

- Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019, September). Factors affecting security behaviour of Kenyan students: an integration of protection motivation theory and theory of planned behaviour. In *2019 IEEE AFRICON* (pp. 1-8). IEEE.
- Fernando, M. S. (2018). IT disaster recovery system to ensure the business continuity of an organization. In *2017 National Information Technology Conference, NITC 2017, 14-15 Sept. 2017, Colombo, Sri Lanka* (pp. 46–48). IEEE.
- Field, A. P. (2005). Is the meta-analysis of correlation coefficients accurate when population correlations vary. *Psychological methods, 10*(4), 444.
- Fink, M. A., & Rothlauf, M. V. (1955). In vitro anaphylaxis in the sensitized mouse uterus. *Proceedings of the Society for Experimental Biology and Medicine, 90*(2), 477-480.
- Freye M, Dennis-Kenji Kipker, Ezekiel Rindstone, Doreen Mwamlangala (2020). Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzania and Germany eHealth system *Datenschutz and Datensicherheit- DuD* June 2020 DOI: 10.1007/S11623-020-1291-3
- Gagneja, KK. (2017). Knowing the ransomware and building defence against it – specific to healthcare institutes. In *Third International Conference on Mobile and Secure Services (MobiSecServ)*, 11-12 Feb, New Orleans. IEEE 1-5.
- Giere, R. N. (2004). How models are used to represent reality. *Philosophy of science, 71*(5), 742-752.

- Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism*, 10(2), 486-489.
- Gyorkos, T. (2003). *Monitoring and Evaluation of large scale Helminth control programmes. Acta Tropic.*
- Glassman, J., Prosch, M and Shao, B. (2015). "To monitor or not to monitor: effectiveness of a cyberloafing countermeasure", *Information & Management*, Vol. 52 No. 2, pp.170-182.
- Glover, G. (2015). *The importance of log management*. Retrieved Jan 29, 2017, from <http://blog.securitymetrics.com/2015/08/importance-of-log-management.html>
- Gupta, M., Charturvedi, A.R., Metha, S and Valeri, L., (2001). "The experimental analysis of information security management issues for online financial services", ICIS 2000, pp.667-75
- Gujarati, D. N. (2003). *Basic Econometrics*. 4th ed. New York: McGraw-Hill.
- Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modelling (PLS-SEM): An emerging tool in business research. *European business review*, 26(2), 106-121.
- Hair, J., Sarstedt, M., Ringle, C., & Hult, G. T. (2017). *A primer on partial least squares structural equation modelling (PLS-SEM) (Second ed.)*. Los Angeles: Sage Publication.
- Hassidim, A., Marciano, D., Romm, A., & Shorrer, R. I. (2017). The mechanism is truthful, why aren't you? *American Economic Review*, 107(5), 220-224

- Hatcher, L., & O'Rourke, N. (2013). *A step-by-step approach to using SAS for factor analysis and structural equation modelling*. Sas Institute.
- Herath & Rao (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*. DOI: 10.1057/ejis.2009.6Corpus ID: 15177006
- Hermawan, T., & Wardhani, R. W. (2017). Implementation AES with digital signature for secure web-based electronic archive. *In 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 5-6 Oct. 2016, Yogyakarta, Indonesia (pp. 1–6). IEEE
- HIPAA, (2015). *General Information*. Available from: <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/> (Accessed 17 March 2020).
- Jacobs, S. (2016). *Engineering Information Security*. Hoboken: Jacobs.
- Jamieson, S. (2004). Likert scales: How to (ab)use them. *Medical Education*, 38(12), 1212-1218. <https://doi.org/10.1111/j.1365-2929.2004.02012.x>
- Kajirunga A., Kalegele K. (2015). Analysis of Activities and Operations in the Current E-HealthL and scape in Tanzania: Focus on Interoperability and Collaboration. (IJCSIS) *International Journal of Computer Science and Information Security*, Vol. 13, No. 6, June 2015. <http://sites.google.com/site/ijcsis/>
- Kamau, G., Boore, C., Maina, E., & Njenga, S. (2018). Block chain technology: Is this the solution to emr interoperability and security issues in developing

- countries? In 2018 *IST-Africa Week Conference (IST-Africa)* (pp. Page-1). IEEE
- Kamoun, F., & Nicho, M. (2014). Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach causation and prevention. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, 9(1), 42-60.
- Kanani G. (2016). Money Matters in Health & Tech: The Road Towards E-Health in Tanzania. *The Citizen Online Magazines* (Monday, November 7, 2016). Retrieved on 08<sup>th</sup> March.2021  
[athttps://www.thecitizen.co.tz/magazine/The-road-towards-e-Health-in-Tanzania/1840564-3443772-format-xhtml-nboinv/index.html](https://www.thecitizen.co.tz/magazine/The-road-towards-e-Health-in-Tanzania/1840564-3443772-format-xhtml-nboinv/index.html)
- Khac Hai N, Lawpoolsri S, Jittamala P, Thi Thu Huong P, Kaewkungwal J. *Practices in security and confidentiality of HIV/ AIDS patients' information: a national survey among staff at HIV outpatient clinics in Vietnam*. PLoS One. 2017;12(11):160–169.
- Kirtley, E. (2018). *What is SIEM? What is SOAR? How are they different?* Retrieved from Swimlane: <https://swimlane.com/blog/siem-soar/>
- Klein, R. H., & Luciano, E. M. (2016). What influences information security behaviour? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management*, 13, 479-496.
- Kline, T. J. B (2005). *Psychological testing: A practical approach to design and evaluation*. Thousand Oaks, California: Sage.



- Kolli, S., Lilly, J., & Wijesekera, D. (2018). Positive Train Control Security: An Intrusion Detection System to Provide Cyber-Situational Awareness. *IEEE Vehicular Technology Magazine*, 13(3), 1–13.
- Kothari, C. (2004). *Research Methodology: Methods & Techniques* (2nd ed.). New Delhi: New Age International (P) Limited, Publishers.
- Kothari, C. R., & Garg, G. (2014). *Research Methods: Methods and Techniques*. New Delhi: New Age International (P) Limited.
- Kouns, J., & Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments*. Hoboken: Wiley.
- Kritzinger, E. and Solms, S. (2013). *A Framework for Cyber Security in Africa*. JIACS, Vol. 3, pp.1-10
- Kumar, V. (2012). *Security Information Management vs Security Event management vs Security Information and Event Management*. Retrieved Dec 23, 2021, from <https://www.symantec.com/connect/articles/security-information-management-vs-security-event-management-vs-security-information>
- Kumar, R. (2014). *Research Methodology: A Step-by-Step Guide for Beginners* (4 edition). SAGE Publications Ltd
- Kvavik, R. B., Voloudakis, J., Caruso, J. B., Katz, R. N., King, P., & Pirani, J. A. (2003). *Information technology security: Governance, strategy, and practice in higher education*. Educause Center for Applied Research. Retrieved from <http://www.educause.edu/ers0305>.

- Kwo-Shing Hong; Yen-Ping Chi; Louis R Chao; Jih-Hsing Tang (2003). An integrated system theory of information security management. *Information Management & Computer Security*; 2003; 11, 5; ABI/INFORM Global pg. 243
- Lampson, B.W. (2004). Computer security in the real world. *Computer*, 37(6), 37-46.
- Ledesma, R. D., & Valero-Mora, P. (2007). *Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis*. *Practical assessment, research & evaluation*, 12(2), 1-11.
- Leech, N. L., Barrett, K. C., & Morgan, G. A. (2015). *IBM SPSS for intermediate statistics: Use and interpretation*. East Sussex: Routledge.
- Line, M. B. (2015). *Understanding Information Security Incident Management Practices, a Case Study in the Electric Power Industry*. PhD Thesis. Norwegian University of Science and Technology. Retrieved from [https://brage.bibsys.no/xmlui/bitstream/id/384795/Line, Maria Bartnes.pdf](https://brage.bibsys.no/xmlui/bitstream/id/384795/Line_Maria_Bartnes.pdf)
- Liu, C. Z., & Kavakli, M. (2018). An Agent-Based Collaborative Information Processing System for Mixed Reality Applications – Part A: Agent-Aware Computing. In 2018 13th IEEE *Conference on Industrial Electronics and Applications (ICIEA)*, 31 May-2 June 2018, Wuhan, China, China (pp. 1273–1278). IEEE
- Lubis, A. R., Fachrizal, F., & Lubis, M. (2018). Wireless Service at Public University: A Survey of Users Perception on Security Aspects. In 2018

*International Conference on Information and Communications Technology (ICOIACT)*, 6-7 March 2018, Yogyakarta Indonesia (pp. 78–83). IEEE.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual review of psychology*, *63*, 539-569.

Magd, H. A. (2008). ISO 9001: 2000 in the Egyptian manufacturing sector: perceptions and perspectives. *International Journal of Quality & Reliability Management*, *25*(2), 173-200.

Mahimane, A. (2013). *Effective Capacity Planning of the Virtual Environment using Enterprise Architecture*. Master Thesis. The Ohio State University. Retrieved from [https://etd.ohiolink.edu/rws\\_etd/document/get/osu1367278818/inline](https://etd.ohiolink.edu/rws_etd/document/get/osu1367278818/inline).

Martin, G, Martin, P, Hankin, C, Darzi, A & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *British Medical Journal* *358*(3): 179.

Martin, S., & Tokutomi, M. (2012). Password cracking. *Computer Security Reports Csc566, University of Arizona*

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*. Sage publications.

Matta, F. K., Scott, B. A., Koopman, J., & Conlon, D. E. (2015). Does seeing “eye to eye” affect work engagement and organizational citizenship behaviour? A role theory perspective on LMX agreement. *Academy of Management Journal*, *58*(6), 1686-1708.

- Maqbool, Z., Aggarwal, P., Pammi, V. S. C., and Dutt, V. (2020). Cyber security: effects of penalizing defenders in cyber-security games via experimentation and computational modelling. *Front. Psychol.* 11:11. doi: 10.3389/fpsyg.2020.00011
- Mbwesa, J. K. (2006). *Introduction to management research*, a student handbook. Nairobi: Jomo Kenyatta Foundation.
- McAfee (2021). *What is endpoint Detection and Response (EDR?)* [Internet]. [place unknown]: McAfee, 2021 available in <https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html>
- Mehrad, A., &Tahriri, M. (2019). Comparison between qualitative and quantitative research approaches: Social sciences. *International Journal for Research in Educational Studies*, 5(7), 1-7.
- Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: the application of security safeguards. *Actainformaticamedica*, 24(1), 47.
- Miles, H., & Huberman, A. M. (2018). Saldana. (2014). *Qualitative data analysis: A methods sourcebook*, 3.
- Miloslavskaya N.G., Senatorov M.Y., Tolstoy A.I. «*Information Security Management Issues*» Series. In 5 volumes. Volume 5: Checks and Assessment of Information Security Activity. Moscow: Goriachajalinia-Telecom. 2014. 2nd edition. 166 p

- Mirza, A. N. (2016). *Analysing error detection performance of checksums in embedded networks*. Master Thesis. Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/4844>
- MOHCDGEC (2017). Tanzania digital health investment road map 2017-2023: *The journey to better data for better health in Tanzania*. Available at <https://www.healthdatacollaborative.org/where-we-work/tanzania/>; [accessed on 16 Jun. 2021]
- Moutinho, L., & Hutcheson, G. (2010). *Statistical Modelling for Business and Management*. *Computing*, 78(73), 1-00.
- Mugenda. &Mugenda, (2003). *Research methods; quantitative and qualitative approaches*: Africa Center for Technology (ACTS), Nairobi Kenya.
- Mugo, DM & Nzuki, D. (2014). Determinants of electronic health in developing countries. *International Journal of Arts and Commerce* 3(3):49-59.
- Morgan, E. (2019). *Cybersecurity Talent Crush to Create 3.5 Million Unfilled Jobs Globally by 2021*. Retrieved from: <https://cybersecurityventures.com/jobs/>
- MoHSW (2009). *Health Sector Strategic Plan III (July 2009–June 2015)*. The United Republic of Tanzania Ministry of Health and Social Welfare: available at <http://ihi.eprints.org/970/1/HealthSectorStrategicPlan.pdf> (accessed February 15, 2021)
- Msumi, M.M. (2018). An Overview of eHealth Regulations in Tanzania. *Datenschutz Datensich* 42, 373–375 (2018). <https://doi.org/10.1007/s11623-018-0959-4>

- Nair, Jayakrishna, MoneerAlshaikh and Christopher Culnane (2020). The scope and functions of health information in e-Health. *Journal of e-Health Management*, DOI: 10.5171/2020.55756
- Nasser, G.; Morrison, B.W.; Bayl-Smith, P.; Taib, R.; Gayed, M.; Wiggins, M.W (2020). *The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails*. *Front. Big Data* 2020,3, 33
- Nehemiah L, N (2014). Towards EHR interoperability in Tanzania hospitals: issues, challenges and opportunities. *International Journal of Computer Science, Engineering and Applications (IJCSEA)* Vol.4, No.4, August 2014
- Neuman, W. L. (2006). *Social research methods: Quantitative and qualitative approaches* (Vol. 13, pp. 26-28). Boston, MA: Allyn and bacon.
- NIST (2011). *Guide for Applying the Risk Management Framework to Federal Information Systems*. Washington, DC: National Institute of Standards and Technology.
- NIST (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. Washington, DC: National Institute of Standards and Technology.
- NIST (2013). *Special publication 800-53 (Rev.4)*. Washington, DC: U.S. Department of Commerce
- NIST. (2017). *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5. Washington, DC: National Institute of Standards and Technology.

- Nisreen Innab (2018). Managing the information security issues of electronic medical records. *International journal of Security, Privacy and Trust Management (IJSPTM)* Vol 7, No ¾ November 2018
- Norman, G. Likert scales (2010). *Levels of measurement and the “laws” of statistics*. *Adv. Health Sci. Educ.* 2010, 15, 625–632
- Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in health sciences education*, 15(5), 625-632.
- Nosworthy J.D. (2000). *Implementing information security in the 21st century – do you have the balancing factors?* *Computers and Security* 2000; 19(4):337–347.
- Pallant, J. (2005). *SPSS Survival Manual: A Step-by-Step Guide to Data Analysis Using SPSS for Windows* (3rd ed.). McGraw-Hill.
- Pallant, J. F., Haines, H. M., Green, P., Toohill, J., Gamble, J., Creedy, D. K., & Fenwick, J. (2016). Assessment of the dimensionality of the Wijma delivery expectancy/experience questionnaire using factor analysis and Rasch analysis. *BMC pregnancy and childbirth*, 16, 1-11.
- Papoutsis, C, Reed, JE, Marston, C Lewis, Majeed, A & Bell, D. 2015. Patient and public views about the security and privacy of electronic health records (EHRs) in the UK: results from a mixed methods study. *BMC Medical Informatics and Decision Making*, 15, 14 October 2015. Available from:<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4607170/> (Accessed 24 June 2020).

- Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, 3(1), 1-8.
- Patton, C., Sawicki, D., & Clark, J. (2015). *Basic methods of policy analysis and planning—pearsonetext*. Routledge.
- Peikari, H. R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC medicalinformatics and decision making*, 18, 1-13.
- Petters J (2021). *IDS vs IPS: What is the difference?* [internet]. [place unknown] available from <https://www.veronis.com/blog/ids-vs-ips>
- Ponemon Institute. (2016). *Sixth annual benchmark study on privacy & security of healthcare data*. Available from: <https://www.ponemon.org/library/sixth-annual-benchmark-studyon-privacy-security-of-healthcare-data-1>  
(Accessed 22 February 2020)
- Ponemon Institute. (2017). *Cost of Data Breach Study: United State*. Available at: <https://ponemon.org/library/2017-cost-of-data-breach-study-united-states>. (Accessed on 22 May 2020)
- Ponemon Institute (2020). *The economic Value of Prevention in the Cyber Security Lifecycle: United State*. Available at: <https://ponemon.org/library/2020-economic-valueof-prevention-cyber-security-lifecycle-united-states>. (Accessed on 22 May 2020)



- Price waterhouse Coopers (PwC). *The Global State of Information Security Survey*. 2014, from <http://www.pwc.com/gx/en/consulting-services/information-security-survey/download>. HTML
- Olok G. T., Yagos W. O. and Ovuga E. (2015). Knowledge and attitudes of doctors towards e-health use in healthcare delivery in government and private hospitals in Northern Uganda: a cross-sectional study. *BMC Medical Informatics and Decision Making* 15:87. DOI 10.1186/s12911-015-0209-8
- Ou Yang, Y. P., Shieh, H. M., Tzeng, G. H., Yen, L., & Chan, C. C. (2011). Combined rough sets with flow graph and formal concept analysis for business aviation decision-making. *Journal of Intelligent Information Systems*, 36, 347-366
- OWASP. (2017). OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. Retrieved July 21, 2021, from [https://www.owasp.org/index.php/Category:OWASP\\_TopTenProject](https://www.owasp.org/index.php/Category:OWASP_TopTenProject)
- Rahim, M. A., &Magner, N. R. (2005). Confirmatory factor analysis of the styles of handling interpersonal conflict: first-order factor model and its invariance across groups. *Journal of applied psychology*, 80(1), 122.
- Rainie, L. (2018). *Americans' complicated feelings about social media in an era of privacy concerns*. Retrieved from Pew Research:<http://www.pewresearch.org/facttank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>

- Rajivan, P., Aharonov- Majar, E., and Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *J. Cyber Secure*. 6: tyaa002.
- Herath, T., & Rao, H.R. (2009). Encouraging information security behaviours in organizations. *Decision Support Systems*, 47, 154-165
- Rezaeighaleh, H., Laurens, R., Zou, C. C., & Model, A. T. (2018). Secure Smart Card Signing with Time-based Digital Signature. In 2018 *International Conference on Computing, Networking and Communications (ICNC)*, 5-8 March 2018, Maui, HI, USA (pp. 182– 187). IEEE.
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security*, 28(8), 816–826. doi: 10.1016/j.cose.2009.05.008
- Robson, C., & McCartan, K. (2016). *Real world research: A resource for users of social research methods in applied settings*
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93. Retrieved from <https://libproxy.library.unt.edu:9443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=5194756&site=ehost-live&scope=site>
- Rothstein, MA & Talbott, MK. (2007). Compelled authorizations for disclosure of health records: magnitude and implications. *American Journal of Bioethics* 7(3): 38-45.
- Rudman, L. (2014). *Analysis of Ntp Based Amplification Ddos Attacks Submitted in partial fulfilment*. PhD Thesis. Grahamstown: Rhodes University

- Runkle, D. E., DeFusco, R. A., Anson, M. J. P., Pinto, J. E., & McLeavey, D. W. (2013). *Quantitative investment analysis*; Hoboken, N.J: Wiley.
- Sabena, D. (2015). *New Test and Fault Tolerance Techniques for Reliability Characterization of Parallel and Reconfigurable Processors*. PhD Thesis. Politenico Di Torino. Retrieved from [http://www.phdauin.polito.it/pdfs/Daive SABENA\\_thesis.pdf](http://www.phdauin.polito.it/pdfs/Daive SABENA_thesis.pdf)
- Saminu Attahiru (2019). A framework for effective information system security management in Katsina State healthcare organizations. *International Journal of Engineering Applied Sciences and Technology*. DO.10.33564/IJEAST. 2019. Vol047.013
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. (5th edition, Ed.). England: Pearson Education Limited.
- Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research methods for business students* (5th ed.). Edinburgh: Pearson Education Limited.
- Saunders, M., Lewis, P. & Thornhill, A. (2012). *Research methods for business students*. (6th ed.). England: Harlow Pearson Educational Limited.
- Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research methods for business students*. Essex: Prentice Hall: Financial Times.
- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B& Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and Operationalization. *Quality & quantity*, 52, 1893-1907.
- Sekaran, U., & Bougie, R., (2010). *Research Methods for Business: A Skill Building Approach* (5th Ed.). West Sussex, UK: John Wiley & Sons Ltd.

- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach*. John Wiley & Sons. <https://doi.org/10.1108/lodj-06-2013-0079>
- Shamsi, J. A., & Khojaye, M. A. (2018). *Understanding privacy violations in big data systems*. *IT Professional*, 20(3), 73–81.
- Schneier, B. (2001). "Managed security monitoring: network security for the 21st Century." *Computers and Security* 20(6): 13.
- Shank, N, Willborn, E, PytlikZillig, L & Noel, H., (2019) Electronic health records: eliciting behavioural health providers' beliefs. *Community Mental Health Journal* 48(2):249-254.
- Shenoy, M. & Madan, P. (2000). *Statistical Methods in Business and Social and Post Graduate Students*. London: Palgrave Macmillan.
- Smith AD. (2008). Biometrics-based service marketing issues: Exploring acceptability and risk factors of iris scans associated with registered travel programmes. *International Journal of Electronic Healthcare* 4:43-66.
- Sittig, DF & Singh, H. (2016). A socio-technical approach to preventing, mitigating and recovering from ransomware attacks. *Applied Clinical Informatics* 7(2): 627-628
- Serge, V. (2006). *A classical introduction to cryptography: applications for communications security*. Springer.
- Siponen, M.T (2000). *A conceptual foundation for organizational information security*

- awareness*. *Information Management & Computer Security*, 2000 8(1): p.31-41
- Stake, R. (2010). *Qualitative research: Studying how things work*. Guilford Press.
- Stevens, S. S. (1946). *On the theory of scales of measurement*. 677-680.
- Stewart, H.; Jürjens, J. (2017). *Information security management and the human aspect in organizations*. *Inf. Computer Security*. 2017, 25, 494–534
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276. Retrieved from <http://pubsonline.informs.org/doi/abs/10.1287/isre.1.3.255>
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441–469.
- Sultan, A., Yang, X., Hussain, S. B., & Hu, W. (2018). Physical -Layer Data Encryption using Chaotic Constellation Rotation in OFDM-PON. In 2018 15th *International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 9-13 Jan. 2021, Islamabad, Pakistan (pp. 7–9). IEEE.
- Sullivan, G. M., & Artino Jr, A. R. (2013). Analyzing and interpreting data from Likert-type scales. *Journal of graduate medical education*, 5(4), 541-542.
- Tabachnick, B. G., & Fidell, L. S. (2014). *Using multivariate statistics*. Harlow. *Essex: Pearson Education Limited*.
- Tanzania Computer Emergency Response Team (2020) *Reports – Tanzania Computer*

*Emergency Response Team*, Available at:

<https://www.tzcert.go.tz/resources-2/reports/> [Accessed: 19 October 2021].

Tanzania Health Enterprise Architecture (TzHEA), version 1 (2020). *Implementation of eHealth* Available at:

<http://hidl.afya.go.tz/#/library/dashboard/document-details/25>. [Assessed 21 November 2021].

Trustwave. (2016). *Trustwave global security report 2016*. Retrieved Nov 13, 2016, From <https://www.info-point 2016.pdf>

University of Illinois Chicago. (2020). *How Secure Is Your Data? Assessing and Mitigating Risks for Electronic Health Records*. Retrieved from <https://healthinformatics.uic.edu/blog/how-secure-is-your-data-assessing-and-mitigating-risks-for-electronic-health-records/>

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., and Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modelling of network attackers, defenders, and users. *Front. Psychol.* 9:691. doi: 10.3389/fpsyg.2018.0069

Vogt, W. P. (2007). *Quantitative research methods for professionals* (pp. 117-118). Boston, MA: Pearson/Allyn and Bacon.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security Management. *Computers & security*, 23(5), 371-376.

Vroom C., Von Solms R. (2004). *Towards information security behavioural compliance*. *Computers and Security* 2004; 23(3):191–198.

- Wadgave, U., &Khairnar, M. R. (2016). Parametric tests for Likert scale: For and against. *Asian journal of psychiatry*, 24, 67-68.
- Wanyonyi, E, Rodrigues, A, Abeka, S &Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International journal of scientific & technology research* 6(12): 47-53.
- Weber, R (1999), *Information System Control and Audit*, Prentice Hall, Englewood Cliffs, NJ. Weidman, G. (2014). *Penetration Testing*. San Francisco: No Starch Press.
- Wilfred, C, (2006). Philosophy, Methodology and action research. *Journal of Philosophy of Education*.
- Willits, F. K., Theodori, G. L., &Luloff, A. E. (2016). Another look at Likert scales. *Journal of Rural Social Sciences*, 31(3), 126.
- Whitman, M., & Mattord, H. (2005). *Principles of Information Security* (2<sup>nd</sup> ed.). Boston, MA: Course Technology
- Wu, DT, Smart, N, Ciemins, EL, Lanham, HJ, Lindberg, C & Zheng, K. (2017). Using EHR audit trail logs to analyse clinical workflow: A case study from community-based ambulatory clinics. *In AMIA Annual Symposium Proceedings of the American Medical Informatics Association* 3(2): 182
- Yamane, Taro. (1967). *Statistics, an introductory analysis* (2nd ed.). New York: Harper and Row.
- Zamir, A., Khan, H. U., Iqbal, T., Yousaf, N., Aslam, F., Anjum, A., &Hamdani, M. (2020). Phishing web site detection using diverse machine learning algorithms. *The Electronic Library*, 38(1), 65-80.

Zeng, X. 2016. The impacts of electronic health record implementation on the healthcare workforce. *North Carolina medical journal* 77(2):112-114.

Zurita, L & Nøhr, C. 2004. *Patient opinion – EHR assessment from the user's perspective*. *Medinfo* 107:1333-1336



## APPENDIX I: Data Collection Tools

Dear Respondent,

My name is Ernest Godson, a PhD candidate at OUT, I hereby invite you to participate freely in the study entitled “*Assessment of the influence of security monitoring practices on security of electronic health records in Tanzanian Public hospitals*”. The respondents targeted by this study are within health professionals in Tanzania public hospitals. You have been selected as a respondent because you fall in one of these categories and we believe you have valuable information necessary for the successful completion of this study. Moreover, although your participation is very important; still, you are free not to participate and you may even withdraw your participation at any time without any negative consequence on your part.

Sincerely yours

---

Ernest Godson

Call: +255764284188

Email: [godsonernest@ymail.com](mailto:godsonernest@ymail.com)

### General instructions:

Please circle the correct answers from the options below in part A

PART A: BACKGROUND INFORMATION (To be filled by all respondents)							
A1	What is your sex?	Male	Female				
		1	2				
A2	In which age category do you fall?	20 – 30	31 – 40	41 – 50	51 – 60	61 and above	
		1	2	3	4	5	
A3	What is your current highest academic qualification?	Certificate	Diploma	Bachelor	Masters	PhD	Prof
		1	2	3	4	5	6
A4	What is your current occupation?	IT Officer	Doctor	Nurse	Pharmacist	Record officer	Others
		1	2	3	4	5	6

**PART B**

**Instruction:** With all the constructs and sub constructs below, please circle the appropriate corresponding number in the columns, which BEST matches your choice

(1 = Strongly disagree; 2= Disagree; 3 = Somehow agree; 4 = Agree; 5 = strongly agree)

S/No.	Statement	Strongly disagree	Disagree	Somehow agree	Agree	Strong Agree
<b>Security Awareness Training</b>						
B1	The hospitals conduct regular security training and awareness to its employees	1	2	3	4	5
B2	The hospital management communicates employees' security roles and responsibilities in an effective manner	1	2	3	4	5
B3	Hospital management encourages users to understand information security policies for effective security of EHR systems	1	2	3	4	5
B4	Hospital conduct training to help employees improve their awareness on phishing and social engineering	1	2	3	4	5
B5	Security awareness training on incident response is a wise approach that decreases the risk of security incidents in EHR systems	1	2	3	4	5
B6	With security awareness training, I convinced other employees to comply with security rules and procedures	1	2	3	4	5
B7	I receive security awareness training on technical measures of security controls in EHRs	1	2	3	4	5
B8	I have enough knowledge on incident response which help me to behave safely in securing EHRs	1	2	3	4	5

S/No.	Statement	Strongly disagree	Disagree	Somewhat agree	Agree	Strong Agree
B9	The security awareness on basic digital-hygiene practices such as the use of strong password helps me to behave safely in security controls of EHRs	1	2	3	4	5
B10	The security awareness helps me to share my knowledge to other employees on new and modern techniques to reduce security incidents in EHRs	1	2	3	4	5
<b>C: Security Controls Assessment</b>						
C1	The hospital has audit trail logs which helps to monitor all access to the system	1	2	3	4	5
C2	The hospital conducts regular risks and vulnerability assessment to know all risks to the system	1	2	3	4	5
C3	The hospital has a system to assess users' adherence to security policies and strategies	1	2	3	4	5
C4	The hospital conducts periodic internal and or external independent system audit to assess its performance	1	2	3	4	5
C5	The hospital performs regular system maintenance and support to improve system performance	1	2	3	4	5
C6	The hospital has employed system quality assurance program to monitor quality of the system	1	2	3	4	5
C7	The hospital has security incident response team to respond on all security incidents	1	2	3	4	5
C8	The hospital has system administrator dedicated for monitoring of security activities only	1	2	3	4	5
C9	The hospital regular review its computer systems and check for misconfiguration for quick response	1	2	3	4	5
C10	The hospital has disaster recovery plan to deals with all system disasters	1	2	3	4	5
C11	The hospital has implemented its security control based on international standard organizations (ISO)	1	2	3	4	5
<b>D: Security Automation</b>						

S/No.	Statement	Strongly disagree	Disagree	Somewhat agree	Agree	Strong Agree
D1	The hospital automatic disabled all unused computers' ports to restrict use of unauthorized personal devices	1	2	3	4	5
D2	The all computers in the hospital have updated antivirus/antispam software to monitor all virus/spams	1	2	3	4	5
D3	The hospital use intrusion detection system (IDS) and intrusion prevention system (IPS)	1	2	3	4	5
D4	The hospital use firewalls for the automatic prevention of intrusions	1	2	3	4	5
D5	The hospital has employed technologies to block or restrict unencrypted sensitive information from traveling to untrusted networks	1	2	3	4	5
D6	The hospital has implemented CCTV camera to monitor its sensitive areas like server rooms	1	2	3	4	5
D7	The hospital uses smart or biometric (e.g., finger print) to access sensitive areas like server rooms)	1	2	3	4	5
D8	The hospital computer automatically set to lock automatically after a few minutes of idle time and require a password to unlock it	1	2	3	4	5
D9	The hospital has automatic off-site backup system as a disaster recovery plan	1	2	3	4	5
<b>E: Behavioural Monitoring</b>						
E1	Users' access right is reviewed at regular interval using formal process	1	2	3	4	5
E2	Users are required to follow good security practices in the use of passwords	1	2	3	4	5
E3	All users return all of the organization's assets upon termination of their employment	1	2	3	4	5
E4	Security rules and policies are enforced by sanctioning the employees who break them	1	2	3	4	5
E5	All employees, contractors and third-party users receive security awareness training	1	2	3	4	5

S/No.	Statement	Strongly disagree	Disagree	Somehow agree	Agree	Strong Agree
E6	Background checks on all candidates for employment, contractors and third party are carried out	1	2	3	4	5
E7	Users are deterred from using information processing facilities for unauthorized purposes	1	2	3	4	5
E8	Users are encouraged to perform regular update of security software	1	2	3	4	5
E9	Repeat security offenders are appropriately disciplined through disciplinary process	1	2	3	4	5
<b>F: Security control of EHR systems</b>						
<b>Confidentiality</b>						
F1	There is a law to work with off-site hospital's ICT facilities	1	2	3	4	5
F2	User's access right to information assets is removed after employment termination	1	2	3	4	5
F3	There is encryption of sensitive information	1	2	3	4	5
F4	There is security confidentiality policy	1	2	3	4	5
F5	There is the use of strong passwords	1	2	3	4	5
<b>Integrity</b>						
F6	There is the use of multi-factor authentication	1	2	3	4	5
F7	In the hospital there is the use of a digital signature	1	2	3	4	5
F8	There is the use of audit trail	1	2	3	4	5
F9	There is rotation of duties among employees	1	2	3	4	5
F10	There is the use of error detect software	1	2	3	4	5
<b>Availability</b>						
F11	There is regular system maintenance	1	2	3	4	5
F12	There is fire extinguisher around all hospital buildings	1	2	3	4	5
F13	The ICT equipment is connected with Uninterrupted Power Supply (UPS)	1	2	3	4	5
F14	There is disaster recovery plan	1	2	3	4	5
F15	There is business continuity plan	1	2	3	4	5

**APPENDIX II: Variable Accuracy Testing**

The study used multiple linear regression analysis. Before using linear regression analysis in conducting primary analysis to meet the research objective and answer the study hypotheses, analysis was performed to assess whether the collected quantitative data met the critical assumptions related to multiple linear regression analysis (Tabachnick and Fidel 2014; Pallant, 2016). The following assumptions were generally assessed, linearity, normality, homoscedasticity and multicollinearity.

**Linearity**

In this study, the linearity test was performed to examine if the relationship between the outcome and predictors variables are linear. The study therefore tested if there was a linear relationship between the predictors (security awareness training, security control assessment, security automation and behavioural monitoring) and outcome variables security controls of EHRs (i.e., confidentiality, integrity and availability) using F-test in the ANOVA table. Testing the hypothesis of no linear relationship between the predictors and dependent variables ( $R\text{-square} = 0$ ) was likewise done. Using the F value to test how well the regression model fitted the data, it was found that the computed F statistics were 6.803, 3.366, 4.346 and 5.084 respectively with an observed significance level of 0.000 i.e., the models reached the statistical significance (Sig. = .000) which was  $p < 0.001$ . Therefore, the hypotheses that there was no linear relationship between the predictors and outcome variables was rejected. Additionally, the residuals had a straight-line relationship with predicted outcome variable scores when referring to the previously given scattered plots

**Table 4. 14    Linearity**

<b>Variable</b>			<b>Sum of Squares</b>	<b>Df</b>	<b>Mean Square</b>	<b>F</b>	<b>Sig.</b>
Security controls of EHRs*	Between Groups	(Combined)	13345.15	33	404.39	6.803	.00
		Linearity	11609.44	1	11609.44	195.30	.00
		Deviation from Linearity	1735.713	32	54.24	.913	.60
	Within Groups		15811.43	266	59.44		
Security controls of EHRs *	Between Groups	(Combined)	9781.87	39	250.81	3.36	.00
		Linearity	6693.97	1	6693.97	89.83	.00
		Deviation from Linearity	3087.90	38	81.26	1.09	.33
	Within Groups		19374.71	260	74.51		
Security controls of EHRs *	Between Groups	(Combined)	9278.73	29	319.95	4.34	.00
		Linearity	7550.63	1	7550.63	102.56	.00
		Deviation from Linearity	1728.09	28	61.71	.83	.70
	Within Groups		19877.85	270	73.62		
Security controls of EHRs *	Between Groups	(Combined)	8387.14	22	381.23	5.08	.00
		Linearity	7016.08	1	7016.08	93.57	.00
		Deviation from Linearity	1371.05	21	65.28	.87	.62
	Within Groups		20769.44	277	74.98		

### Normality

After doing a descriptive analysis, the variables' normality was tested. The dependent variable need to be normal distributed to do inferential analysis such as correlation, regression, or related linear techniques. Before conducting further research, normality must be established if the dependent variable is not normally distributed (Anthony, 2007; Annette, 2002; Alan, 2003). Hair et al. (2010) stated that the actual degree of departure from normalcy can be determined using both graphical representations and statistical tests (Shapiro-Wilk or Kolmogorov-Smirnov tests). Using the Kolmogorov-Smirnov (Shapiro and Wilk, 1965) computed for each variable, the distribution's shape was ascertained. These tests' findings (Table 4.7) indicated that all variables were not significant, proving that the assumption of

normality was met. Also, Figure 4.8 to Figure 4.12 in appendix two indicated that the variables were normally distributed.

**Table 4. 15 Tests of Normality**

<b>Indicator</b>	<b>Kolmogorov-Smirnov</b>			<b>Shapiro-Wilk</b>		
	<b>Statistic</b>	<b>Df</b>	<b>Sig.</b>	<b>Statistic</b>	<b>Df</b>	<b>Sig.</b>
Security awareness	.086	300	.000	.985	300	.004
Security assessment	.082	300	.000	.979	300	.000
Security automation	.134	300	.000	.950	300	.000
Behavioural monitoring	.077	300	.000	.981	300	.001

a. Lilliefors Significance Correction

### **Homoscedasticity**

Homoscedasticity of variances suggests that the dependent variable exhibited the same degree of variability for each value of the predictors variables Beisland, (2014). A homoscedasticity test was performed to test the variance of the residuals of the regression model used. The distribution is normal if the error terms have equal variances. Heteroscedasticity is the term used to describe the unequal variability of the values of the independent variables. The following lists the null and alternative hypotheses. Ho: The data's variance is homogeneous; H1: The data's variance is heterogeneous. According to the rule, Ho is accepted and H1 is refused if the p-value is larger than 0.05; however, Ho is rejected and H1 is accepted if the p-value is less than 0.05. Homogeneity of variances tests for two scale variables are best tested graphically or using statistical tests. The homoscedasticity assumption was tested using the Levene homoscedasticity statistic. Table 4.8 shows that testing at the 0.05 level of significance, none of the Levene statistics was significant. Therefore, the assumption of homoscedasticity was not infringed.



**Table 4. 16 Homoscedasticity**

Indicator	Levene statistic	Df1	Df2	Sig
Security awareness	2.629	1	324	0.000
Security assessment	1.434	1	324	0.000
Security automation	.482	1	324	0.000
Behavioural monitoring	1.343	1	324	0.049

### **Multicollinearity**

In multiple regression model, multicollinearity happens when two or more independent variables are significantly associated (Bickel, 2007). The model will be recognized unless perfect multicollinearity is present, which is all that is required by the Gauss-Markov assumption. Accordingly, the standard errors are accurate and effective, the model can estimate all of the coefficients, and the coefficients keep their best linear and unbiased estimates (Runkle et al., 2013). Multiple regression models' issues with multicollinearity were measured with the use of variance inflation factor (VIF). The VIF statistic for the model's predictors measures how great the error variance is in comparison to the predictor's intrinsic effect (Baguley, 2012).

Cohen and Cleveland (2013) define the variance inflation factor (VIF) as a measure of the amount by which the variance of each regression coefficient increases compared to the situation where all predictors are uncorrelated and suggest a VIF of 10 or greater as a rule of thumb to conclude that the VIF is too large to be appropriate. Runkle et al. (2013) argued that if two or more variables have a variance inflation factor (VIF) greater than or equal to 5, one should be removed from the

regression analysis to indicate the presence of multicollinearity. A VIF value of 4 was assumed as the threshold in this study.

High multicollinearity is indicated when the cross-correlation between the independent variables exceeds 0.9 (cited by Hair et al, 2006, Saunders et al.2009), 0.8 (Garson, 2013), 0.7 (Sakaran & Bougie, 2010), or when the R-squared and significant F-tests of the model are combined with non-significant t-tests. Co-efficiency appearance. For this study, if more than one variable has a coefficient of variance expansion greater than or equal to 5, one should be eliminated from the model. The VIF values in Table 4.9 are less than 5, indicating no statistically significant multicollinearity between the independent variables, as no variables were noted. This meant that there was no multicollinearity, which made the study more pertinent, as advised by Hamilton (2012).

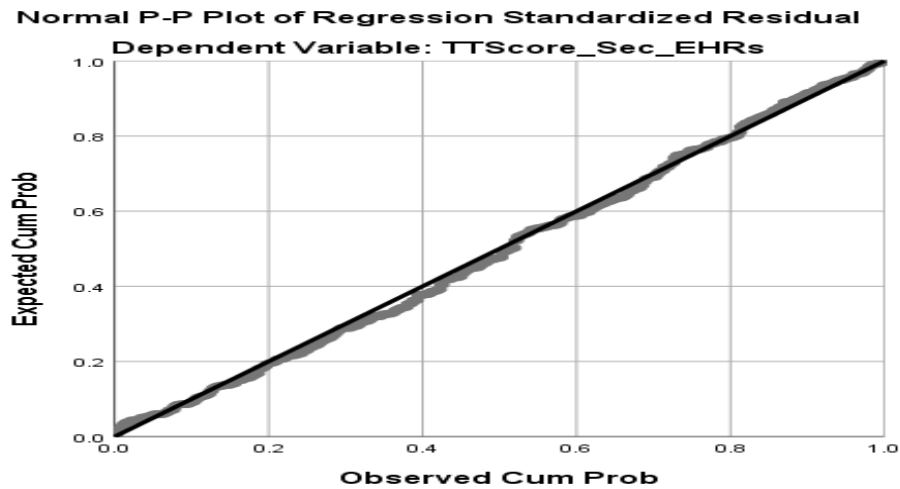
**Table 4.17 Collinearity Statistics**

<b>Indicator</b>	<b>Tolerance</b>	<b>VIF</b>
Security awareness	.729	1.371
Security assessment	.634	1.577
Security automation	.882	1.133
Behavioural monitoring	.591	1.692

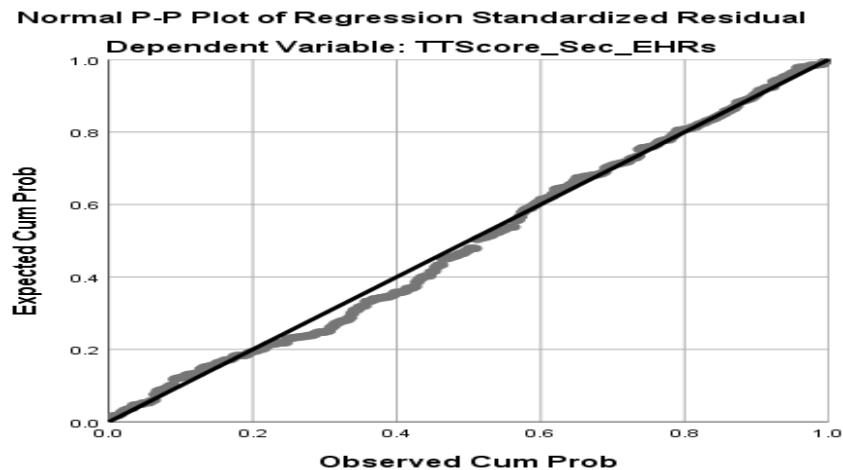
a. Dependent Variable: Security controls of EHRs

## Outliers

The study assessed for outliers in the data set of the variable of the study. The assumption of outliers was not violated in the study as no cases displayed of more than 3.3 or less than -3.3 when referring to the Scatterplot given in Appendix two (Figure 4.12-4.15).



**Figure 4.2 Normal probability Plots for Security Awareness Training**



**Figure 4.3 Normal probability Plots for Security Controls Assessment**

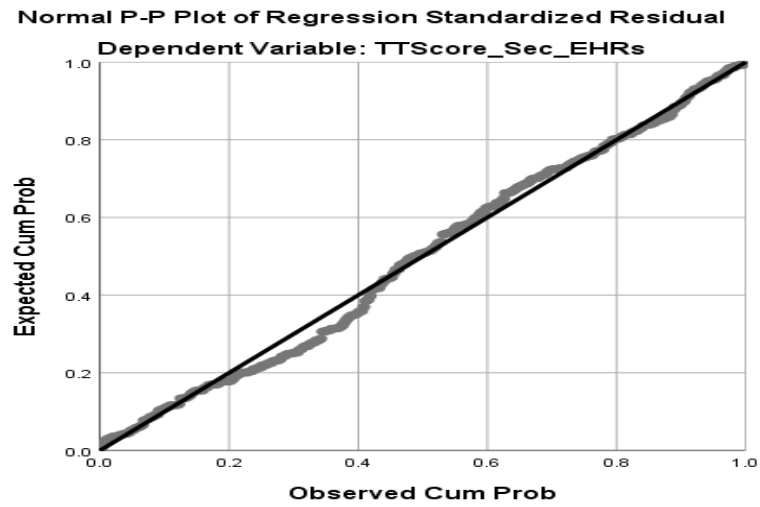


Figure 4.4 Normal probability Plots for Security Automation

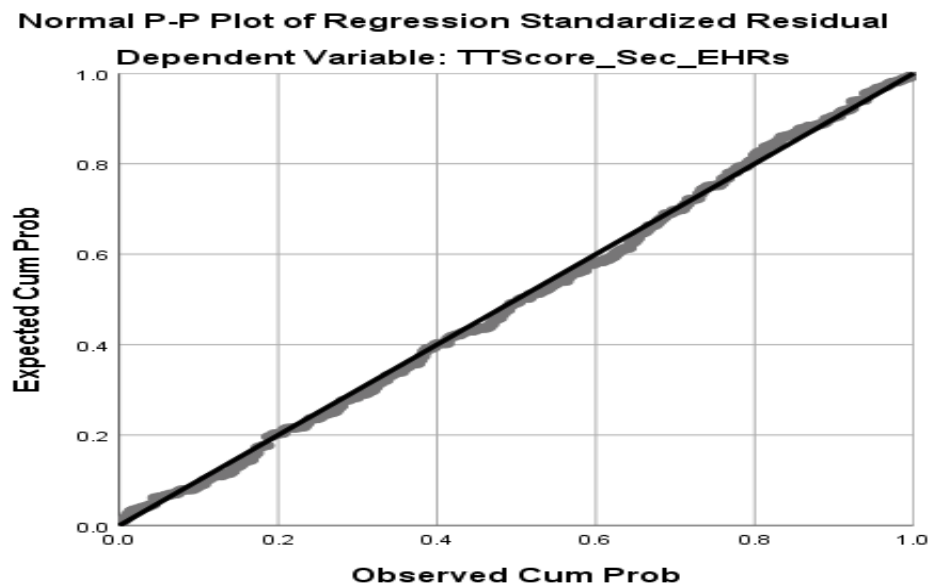
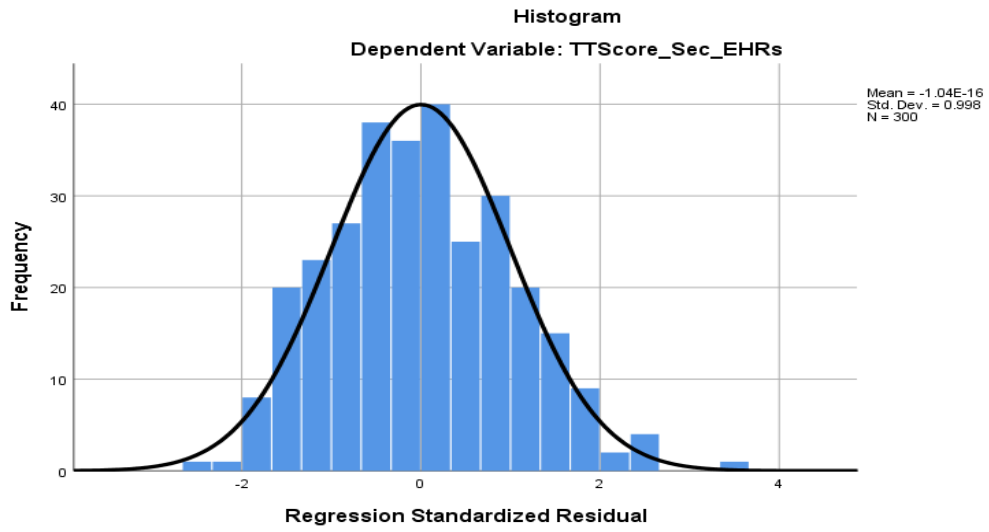
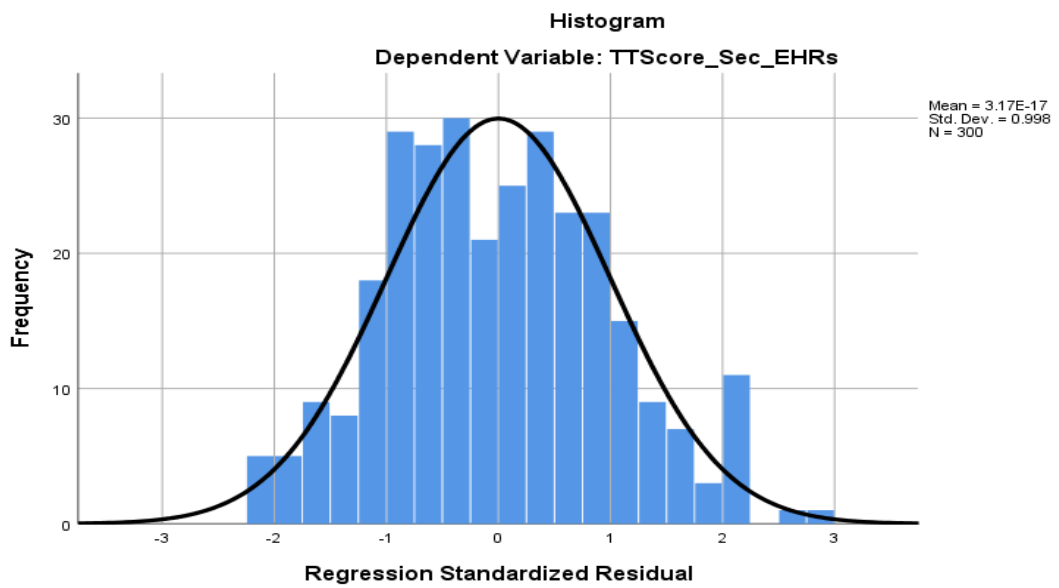


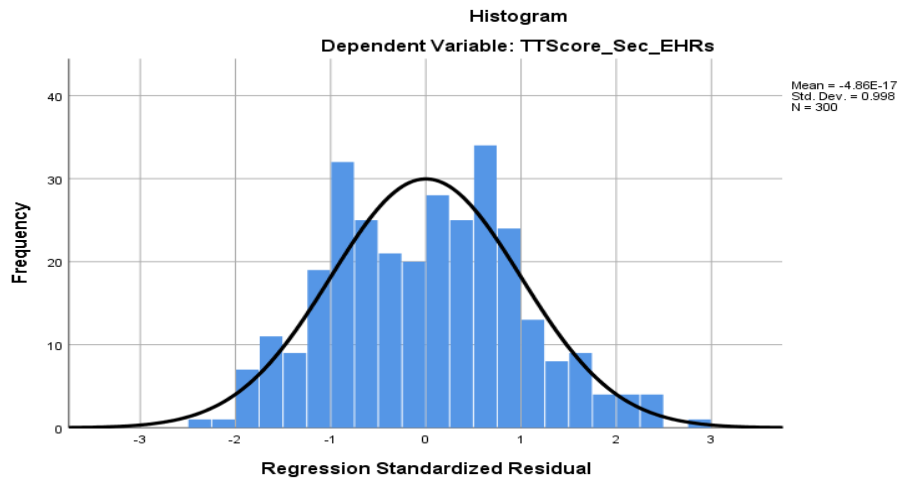
Figure 4.5 Normal probability Plots Behavioural Monitoring



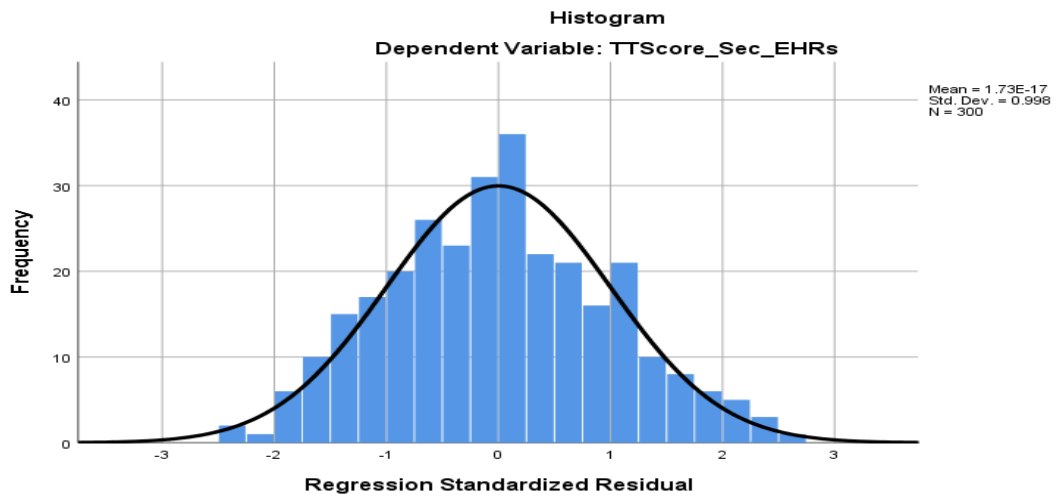
**Figure 4.6 Histograms for Security Awareness Training**



**Figure 4.7 Histograms for Security Controls Assessment**



**Figure 4.8 Histograms for Information Security Automation**



**Figure 4.9 Histograms for Behavioural Monitoring**

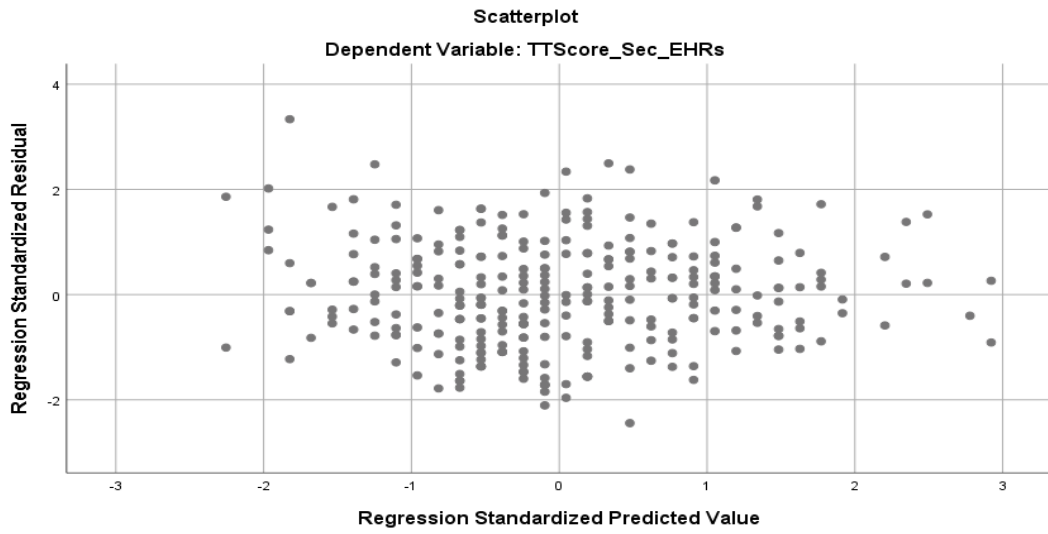


Figure 4.10 Scattered plots for Security Awareness Training

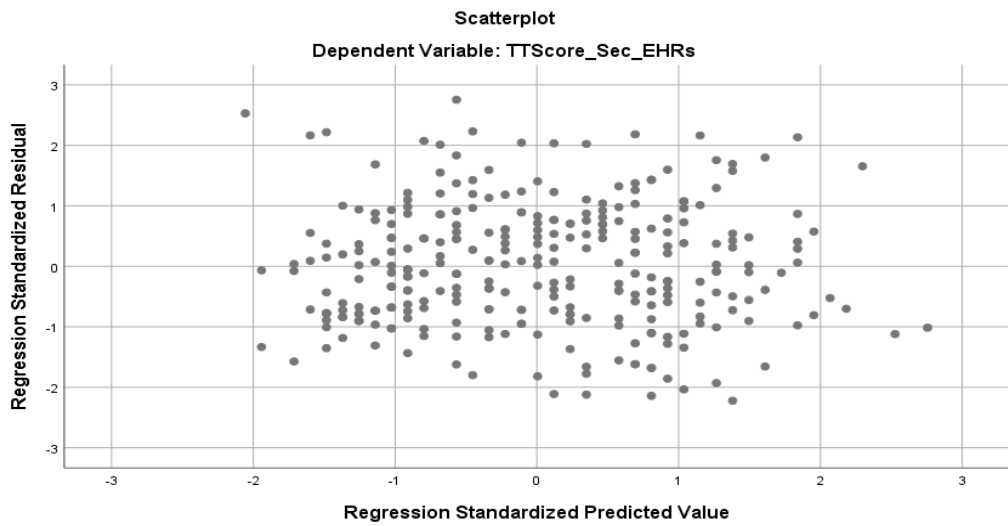
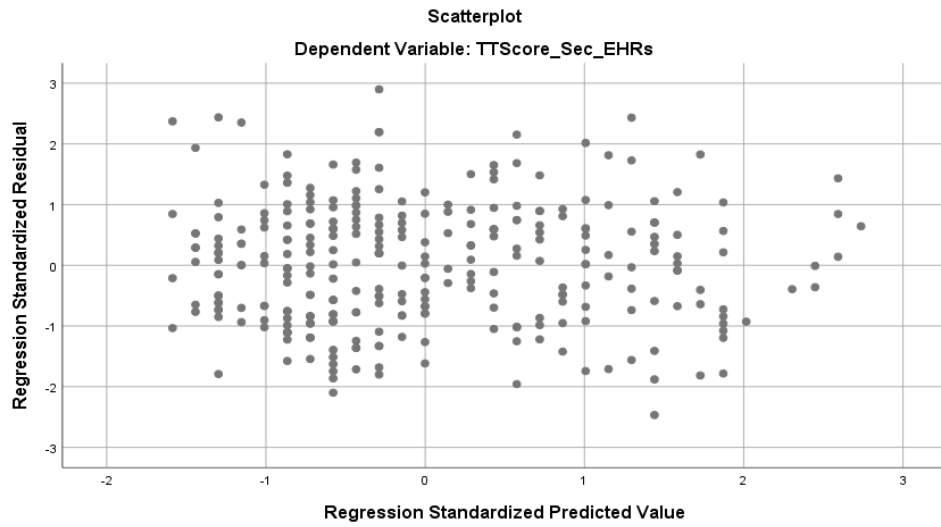
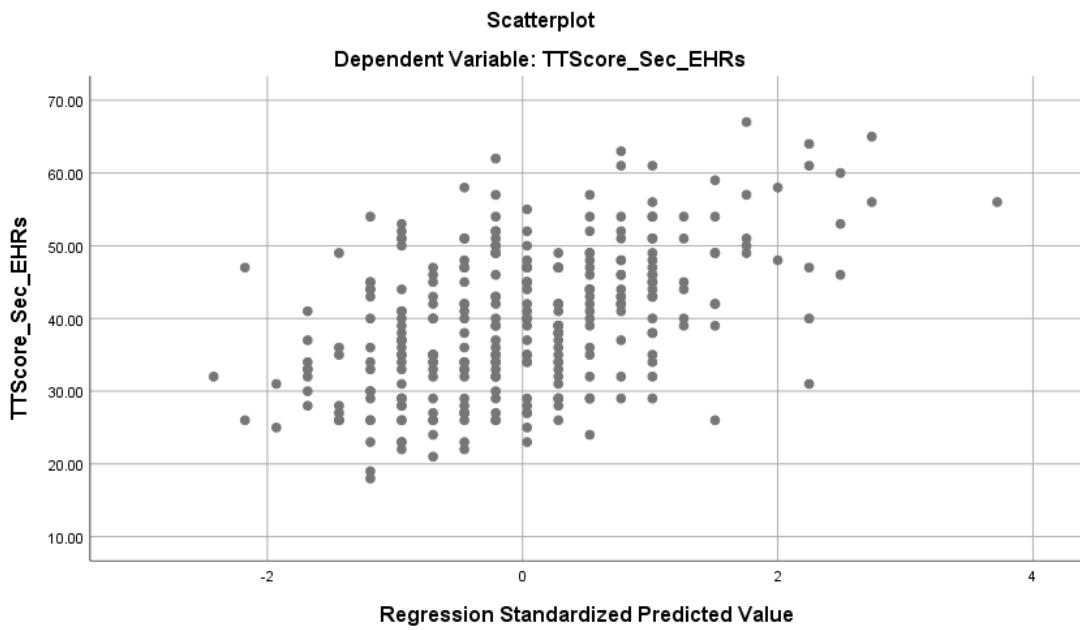


Figure 4.11 Scattered plots for Security Controls Assessment



**Figure 4.12** Scattered plots for Security Automation



**Figure 4.13** Scattered plots for Behavioural Monitoring



### **APPENDIX III: Factor Analysis Results**

In performing factor analysis of this study, three steps were followed: assessment of the appropriateness of the data for factor analysis, factor extraction and factor rotation and interpretation Pallant (2005). In assessing the suitability (Whether Factor analysis was appropriate) of the data for factor analysis, the correlation matrix for a coefficient of 0.3 and above were considered such as the strength of inter-correlations among all items for all the variables of this study which was inspected using correlation matrix for evidence of coefficients greater than 0.3 Tabachnick and Fidell (2001).

Furthermore, the Kaiser-Meyer-Olkin Measure of sampling Adequacy Kaiser (1974) of the minimum value of 0.5 was considered and the Bartlett's test of sphericity was considered significant at ( $p < 0.05$ ). The items considered for interpretation after performing factor rotation were the ones with only loading scores of 0.5 or above and those not cross-loaded during the factor analysis process. The study uses Cronbach's alpha coefficient of a scale of a minimum of 0.7 for the scale with items more than 10 Nunnally (1978) and optimum mean inter-item correlation values range from 0.2 to 0.4 as suggested by Briggs and Cheek (1986) for the scale with items less than 10.

In factor analysis for security awareness, the first component explained 52.365% of the overall variation while the second factor explained 72.007% of the overall variation. In addition, the Kaiser-Meier-Orkin measurement (KMO measurement) was used in this study to test the adequacy of sampling. The results in Appendix two in Table 4.15 of this report show that the KMO was greater than 0.5 and the Bartlett test is significant. Further, on security assessment, the first factor accounted for

73.305% of the total variance and the second factor accounted for 80.760% of the total variance. In addition, the Kaiser-Meier-Orkin measurement (KMO measurement) was used in this study to test the adequacy of sampling. The results in appendix two Table 4.16 show that the KMO was greater than 0.5 and the Bartlett test is significant.

Moreover, the security automation factor analysis revealed that the five component explained 73.254% of the overall variation while the second factor explained 83.120% of the overall variance. In addition, the study tested the accuracy of sampling using the Kaiser-Meier-Orkin measurement (KMO measurement). The results in appendix two's Table 4.17 demonstrate that the Bartlett test is significant and the KMO was greater than 0.5. In addition, the findings of the factor analysis on behavioural monitoring showed that the first component explained 57.408% of the total variation and the second factor explained 91.097%. In addition, the study tested the appropriateness of the sampling using the Kaiser- Meyer- Olkin Measure (KMO measure). Appendix two's findings in Table 4.18 showed that the KMO.

**Table 4.11 Factor analysis for security assessment**

<b>Statement</b>	<b>Factor Loading</b>
<b>SA1:</b> The hospital has audit trail logs which to monitor all access to the system	.903
<b>SA2:</b> The hospital conducts regular risks and vulnerability assessment	.838
<b>SA3:</b> The hospital has a system to assess users' adherence to security policies	.693
<b>ST4:</b> The hospital conducts periodic internal and or external independent system audit review	.936
<b>SA5:</b> The hospital performs regular system maintenance and support to improve system performance	.962
<b>SA6:</b> The hospital has employed system quality assurance to monitor quality	.579
<b>SA7:</b> The hospital has security incident response team to respond on all security Incidents	.526
<b>SA8:</b> The hospital has system administrator dedicated for monitoring of security Activities	.593
<b>SA9:</b> The hospital regular review its computer systems and check for Misconfiguration	.406
<b>SA10:</b> The hospital has disaster recovery plan to deals with all system disasters	.608
<b>SA11:</b> The hospital has implemented its security control based on international standard (ISO)	.922
<b><i>Total variance explained: Rotation sums of squared loadings</i></b>	
Total	3.694
% of Variance	73.305
Cumulative %	73.305
<b><i>KMO and Bartlett's Test</i></b>	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.749
Bartlett's Test of Sphericity, Approx. Chi-Square	2769.805
Df	66
Sig	0.000
Extraction Method: Principal Component Analysis	
Rotation Method: Varimax with Kaiser Normalization	

**Table 4.12 Factor Analysis for Security awareness training**

<b>Statement</b>	<b>Factor Loading</b>
<b>ST1:</b> The hospital conducts regular security training and awareness to its employees	.544
<b>ST2:</b> The hospital management communicates employees' security roles and responsibilities in an effective manner	.708
<b>ST3:</b> Hospital management encourages users to understand information security policies for effective security of EHR systems	.450
<b>ST4:</b> Hospital conduct training to help employees improve their awareness on phishing and social engineering	.584
<b>ST5:</b> Security awareness training on incident response is a wise approach that decreases the risk of security incidents in EHR systems	.554
<b>ST6:</b> With security awareness training, I convinced other employees to comply with security rules and procedures	.384
<b>ST7:</b> I receive security awareness training on technical measures of security controls in EHRs	.595
<b>ST8:</b> I have enough knowledge on incident response which help me to behave safely in securing EHRs	.650
<b>ST9:</b> The security awareness on basic digital-hygiene practices such as the use of strong password helps me to behave safely in security controls of EHRs	.717
<b>ST10:</b> The security awareness helps me to share my knowledge to other employees on new and modern techniques to reduce security incidents in EHRs	.350
<b>Total variance explained: Rotation sums of squared loadings</b>	
Total	1.795
% of Variance	52.365
Cumulative %	52.365
<b>KMO and Bartlett's Test</b>	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	5.78
Bartlett's Test of Sphericity, Approx. Chi-Square	148.184
Df	45
Sig.	0.000
Extraction Method: Principal Component Analysis	
Rotation Method: Varimax with Kaiser Normalization	

**Table 4:13 Factor Analysis for security automation**

Statement	Factor Loading
<b>SAM1:</b> The hospital automatic disabled all unused computers' ports to restrict use of unauthorized devices	.863
<b>SAM2:</b> The all computers in the hospital have updated antivirus/antispam software	.643
<b>SAM3:</b> The hospital use intrusion detection system (IDS) and intrusion prevention system (IPS)	.872
<b>SAM4:</b> The hospital use firewalls for the automatic prevention of intrusions	.921
<b>SAM5:</b> The hospital automatic off-site backup system as a disaster recovery plan	.471
<b>SAM6:</b> The hospital has employed technologies to block or restrict unencrypted sensitive Information	.606
<b>SAM7:</b> The hospital has implemented CCTV camera to monitor its sensitive areas	.771
<b>SAM8:</b> The hospital computers automatically set to lock after a few minutes of idleness	.761
<b>SAM9:</b> The hospital uses smart or biometric (e.g., finger print) to access sensitive areas	.684
 <b>Total variance explained: Rotation sums of squared loadings</b>	
Total	4.032
% of Variance	73.254
Cumulative %	73.254
 <b>KMO and Bartlett's Test</b>	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.802
Bartlett's Test of Sphericity, Approx. Chi-Square	1789.867
Df	36
Sig.	0.000

Extraction Method: Principal Component Analysis

Rotation Method: Varimax with Kaiser Normalization

**Table 4.14 Factor Analysis for Behavioural Monitoring**

<b>Statement</b>	<b>Factor Loading</b>
<b>BM1:</b> Users' access right is reviewed at regular interval using formal process	.547
<b>BM2:</b> Users are required to follow good security practices in the use of passwords	.738
<b>BM3:</b> All users return all of the organization's assets upon termination of their employment	.685
<b>BM4:</b> Security rules and policies are enforced by sanctioning the employees who break them	.587
<b>BM5:</b> All employees, contractors and third-party users receive security awareness training	.511
<b>BM6:</b> Background checks on all candidates for employment, contractors and third party are carried out	.740
<b>BM7:</b> Users are deterred from using information processing facilities for unauthorized purposes	.479
<b>BM8:</b> Repeat security offenders are appropriately disciplined through disciplinary process	.605
 <b><i>Total variance explained: Rotation sums of squared loadings</i></b>	
Total	1.353
% of Variance	57.408
Cumulative %	57.408
 <b><i>KMO and Bartlett's Test</i></b>	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.512
Bartlett's Test of Sphericity, Approx. Chi-Square	41.664
Df	28
Sig.	0.047
<hr/>	
Extraction Method: Principal Component Analysis	
Rotation Method: Varimax with Kaiser Normalization	

## APPENDIX IV: Research Clearance Letters - OUT

### THE OPEN UNIVERSITY OF TANZANIA

#### DIRECTORATE OF POSTGRADUATE STUDIES

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Medical Officer in Charge  
Maweni Regional Referral Hospital  
P.O. BOX 16  
**KIGOMA.**

#### RE: RESEARCH CLEARANCE

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** (No: **PG201902367**) pursuing **PhD**. We here by grant this clearance to conduct a research titled "*Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals*". He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**

**THE OPEN UNIVERSITY OF TANZANIA**

***DIRECTORATE OF POSTGRADUATE STUDIES***

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Medical Officer in Charge  
Iringa Regional Referral Hospital  
P.O BOX 260  
**IRINGA.**

**RE: RESEARCH CLEARANCE**

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** No: **PG201902367** pursuing **PhD**. We here by grant this clearance to conduct a research titled "*Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals*". He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**



**THE OPEN UNIVERSITY OF TANZANIA**

***DIRECTORATE OF POSTGRADUATE STUDIES***

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Executive Director,  
Temeke Referral Hospital,  
P.O BOX 45232,  
**DAR ES SALAAM.**

**RE: RESEARCH CLEARANCE**

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** No: **PG201902367** pursuing **PhD**. We here by grant this clearance to conduct a research titled "*Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals*". He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**

**THE OPEN UNIVERSITY OF TANZANIA**

***DIRECTORATE OF POSTGRADUATE STUDIES***

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Medical Officer in Charge,  
Sekou Toure Regional Referral Hospital,  
P.O BOX 132,  
**MWANZA.**

**RE: RESEARCH CLEARANCE**

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** No: **PG201902367** pursuing **PhD**. We here by grant this clearance to conduct a research titled "**Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals**". He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**

**THE OPEN UNIVERSITY OF TANZANIA**

***DIRECTORATE OF POSTGRADUATE STUDIES***

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Medical Officer in Charge  
Mount Meru Regional Referral Hospital  
P.O BOX 3092  
**ARUSHA.**

**RE: RESEARCH CLEARANCE**

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** (No: **PG201902367**) pursuing **PhD**. We here by grant this clearance to conduct a research titled "*Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals*". He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**

**THE OPEN UNIVERSITY OF TANZANIA**

***DIRECTORATE OF POSTGRADUATE STUDIES***

P.O. Box 23409  
Dar es Salaam, Tanzania  
<http://www.out.ac.tz>



Tel: 255-22-2668992/2668445  
ext.2101  
Fax: 255-22-2668759  
E-mail: [dpgs@out.ac.tz](mailto:dpgs@out.ac.tz)

20<sup>th</sup> June, 2022

**REF: PG201902367**

Medical Officer in Charge  
Dodoma Regional Referral Hospital  
P.O BOX 904  
**DODOMA**

**RE: RESEARCH CLEARANCE**

The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1<sup>st</sup> 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 1<sup>st</sup> January 2007. In line with the Charter, the Open University mission is to generate and apply knowledge through research.

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 **Mr. Ernest Godson** (No: **PG201902367**) pursuing **PhD**. We here by grant this clearance to conduct a research titled **"Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals"**. He will collect his data in your hospital between 15<sup>th</sup> June to December, 2022.

In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly, thank you in advance for your assumed cooperation and facilitation of this research academic activity.


Yours Sincerely,

Prof. Magreth S. Bushesha  
**For: VICE CHANCELLOR**  
**THE OPEN UNIVERSITY OF TANZANIA**

## APPENDIX V: Data Collection Acceptance Letters

**JAMHURI YA MUUNGANO WA TANZANIA  
WIZARA YA AFYA**

Mkoa wa Kigoma:  
Tel: "REGCOM"  
Simu: 028-2802287/2330  
Fax: 028-2802330  
Email: mawenirrh@kigoma.go.tz  
**Unapojibu tafadhali taja**  
KUMB: NA. HAD.73/274/OIE/




Hospitali ya rufaa ya mkoa,  
S. L. P. 16,  
KIGOMA.  
29/6/2022

Mkuu wa Chuo,  
Chuo Kikuu huria cha Tanzania,  
S.L.P. 23409,  
Dar Es Salaam

**YAH: MAOMBI YA KUKUSANYA DATA KATIKA HOSPITALI YA RUFAA YA MKOA  
KIGOMA.**

Husika na mada tajwa hapo juu.

1. Rejea barua yako ya tarehe **20 June, 2022** yenye kumb Na. **PG201902367** iliyopokelewa katika hospitali ya Rufaa ya Mkoa, inayohusu mada tarjwa hapo juu.
2. Napenda kukutarifu kuwa maombi yako ya kukusanya data kuhusu "Information security Electronics Health Records Manageme.it in Tanzania public Hospitals" katika hospitali ya Rufaa ya Mkoa Maweni kwa mwanafunzi **Ernest Godson** mwenye namba ya usajiri (**PG201902367**) yamekubaliwa.
3. Kwa barua hii uongozi wa hospitali unatoa kibai ili aweze kukusanya taarifa anazozihitaji.
4. Nakutakia ushirikiano mwema.

  
Ayub Charles  
Kny: Mganga Mfawidhi (RRH)  
Kigoma

**MGANGA MFAWIDHI  
Kny. HOSPITALI YA RUFAA YA MAWENI  
KIGOMA**

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF HEALTH

**IRINGA REGIONAL**

Phone No.: 026 - 2702264

Fax: 026 – 2702264

Email: [iringarrh@afya.go.tz](mailto:iringarrh@afya.go.tz)

Reply please quote:



Medical Officer In Charge,  
Iringa Regional Referral Hospital  
Kinondoni Street  
P.O. Box 260,  
**IRINGA**

Ref.No. IRRH/E.10/16/Vol. XXXIII/38

24<sup>th</sup> June, 2022

Mr. Ernest Godson  
The Open University of Tanzania,  
P. O. Box 259,  
**DODOMA**

**REF: PERMISSION TO CONDUCT RESEARCH ON "INFORMATION SECURITY CONTROLS ON ELECTRONIC HEALTH RECORDS MANAGEMENT IN TANZANIA PUBLIC HOSPITALS"**

Refer to the heading captioned above and a letter with **Ref. No.** PG201902367 dated 20<sup>th</sup> June, 2022.

2. I am glad to inform you that permission has been granted to conduct your research titled Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals attending Iringa Regional Referral Hospital between 15<sup>th</sup> June to December, 2022.

3. It is my sincere hope that ethical issues and Hospital protocols shall be observed.



Hussein Said  
For: Medical Officer Incharge  
Iringa Regional Referral Hospital  
**IRINGA**

**Copy to:** Office of the Vice Chancellor,  
The Open University of Tanzania,  
P. O. Box 23409,  
**DODOMA**





**JAMHURI YA MUUNGANO WA TANZANIA**  
**WIZARA YA AFYA.**  
**HOSPITAL YA RUFAA YA MKOA YA TEMEKE**



Baruapepe:temekerh@afya.go.tz,S.L.P 45232 Dar es Salaam,Simu 0222856007

Kumb. Na. TRRH/RSC/9/8/54

Tarehe: 11/07/2022

Ndg. Ernest Godson,  
 Chuo Kikuu Huria Tanzania (The Open University)  
 S.L.P 23409  
**DAR ES SALAAM.**

**YAH: OMBI LA KUFANYA UTAFITI KUHUSU "INFORMATION SECURITY  
 CONTROLS ON ELECTRONIC HEALTH RECORDS MANAGEMENT IN TANZANIA  
 PUBLIC HOSPITALS" (RESEARCH)**

Tafadhali husika na somo tajwa hapo juu.

Nimepokea barua yako ya tarehe **20 Juni, 2022** kuhusu ombi lako la kufanya Utafiti (Research) katika Taasisi yetu, kuhusu **"Information Security Controls on Electronic Health Records Management in Tanzania Public Hospitals"**.

Ombi lako limekubaliwa, utatakiwa kulipa ada ya utafiti kiasi cha Tshs. **100,000/=** kwa mwezi mmoja. Hivyo wasiliana na mhasibu wa mapato wa Hospitali **Ndg. Deogratias Tillya** kwa namba **0765 000160** ili akupatie control Number kwa ajili ya malipo ya ada hii ili uweze kuruhusiwa kufanya utafiti.

Asante kwa ushirikiano.



Dr. Husna Msangi  
 Kny: **MKURUGENZI**

**HOSPITALI YA RUFAA YA MKOA YA TEMEKE**

Nakala: **Mhasibu wa Mapato**

**Kiongozi wa (CSCO)**

- **Tafadhali hakikisha taarifa ya utafiti inabaki hospitalini**

## MINISTRY OF HEALTH

MWANZA REGION:

Tel. Address: **"HEALTH"** MWANZA  
 Tel. No: 028-2502171  
 Fax: 028-850  
 Email: sekoutourerrh@afya.go.tz



Sekou Toure Regional Referral Hospital,  
 P.O.Box 132,  
**MWANZA.**

In reply please quote:

Ref. No. FA.137/264/0IL/21

27<sup>th</sup> June, 2022

Mr. Ernest Godson,  
 THE OPEN UNIVERSITY OF TANZANIA,  
 P.O. Box 23409,  
**DAR ES SALAAM.**

Re: **PERMISSION TO CONDUCT REASARCH AT SEKOU TOURE HOSPITAL IN  
 MWANZA**

Kindly refers our letter dated 20<sup>th</sup> June, 2022 reference number REF: PG  
 201902367.

2. I am pleased to inform you that the hospital research board has granted you an approval to conduct the study titled **"INFORMATION SECURITY CONTROLS ON ELECTRONIC HEALTH RECORDS MANAGEMENT IN TANZANIA PUBLIC HOSPITALS"**.
3. You are supposed to share the results of your study to hospital administration.
4. Best regards.

Dr. Bahati Msaki  
**MEDICAL OFFICER INCHARGE (H)  
 MWANZA**





**THE UNITED REPUBLIC OF TANZANIA  
MINISTRY OF HEALTH**

Telegrams: **"REGCOM"**  
Telephone: 250-335751 -2  
Fax: 2544904  
Website: [www.arusha.go.tz](http://www.arusha.go.tz)  
E-mail: [mt.merurrrh@afya.go.tz](mailto:mt.merurrrh@afya.go.tz)  
**In reply please quote:**



REGIONAL REFERRAL HOSPITAL,  
P.O. Box 3092,  
**ARUSHA.**

Ref. No.RMO/AR/F1/15 C/69

14/03/2023

ERNEST GODSON  
P.O. Box 259  
**DODOMA.**

**RE: PERMISSION TO CONDUCT RESEARCH IN OUR HOSPITAL**

Refer to the above heading.

Reference is made as per your letter dated 24 June, 2022 concern the above heading.

The permission is granted to conduct research with title "INFORMATION SECURITY CONTROLS ON ELECTRONIC HEALTH RECORDS MANAGEMENT IN TANZANIA PUBLIC HOSPITALS".

Our Hospital will give all necessary support to the research assistant to enable them to full fill their objectives.

Best regards.

A handwritten signature in blue ink, appearing to read 'Gerald Philip'.

Gerald Philip  
**For: MEDICAL OFFICER INCHARGE  
MT. MERU RRH  
ARUSHA.**



UNITED REPUBLIC OF TANZANIA  
Ministry of Health

Telegram: "Alya" 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.22/130/03/37

29/07/2022

Ernest Godson,  
The Open University,  
P. O. Box 23409,  
DAR-ES-SALAAM.

**RE: ACCEPTANCE FOR RESEARCH INFORMATION SECURITY  
CONTROLS ON ELECTRONIC HEALTH RECORDS MANAGEMENT IN  
TANZANIA PUBLIC HOSPITALS.**

The heading above is concerned.

I would like to inform that your request for Research studies in Dodoma Regional Referral Hospital has been received and accepted with cost implication during the whole period of research.

Please note that you are suppose to follow all rules and Regulations which guide the Hospital.

Thank you,

FOR: MEDICAL OFFICER INCHARGE  
DODOMA REGIONAL REFERRAL HOSPITAL  
P. O. BOX 904 DODOMA KOSRW

Maxmillian Tryphone  
FOR, MEDICAL OFFICER INCHARGE  
DODOMA