SECURITY OF ELECTRONIC PERSONAL HEALTH INFORMATION IN A PUBLIC HOSPITAL IN SOUTH AFRICA

By

Kabelo Given Chuma

[Student No. 50119869]

Submitted in accordance with the requirements for the degree of

MASTER OF INFORMATION SCIENCE

in the subject

INFORMATION SECURITY

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR M NGOEPE

JANUARY 2020

ABSTRACT

The adoption of digital health technologies has dramatically changed the healthcare sector landscape and thus generates new opportunities to collect, capture, store, access and retrieve electronic personal health information (ePHI). With the introduction of digital health technologies and the digitisation of health data, an increasing number of hospitals and peripheral health facilities across the globe are transitioning from a paper-based environment to an electronic or paper-light environment. However, the growing use of digital health technologies within healthcare facilities has caused ePHI to be exposed to a variety of threats such as cyber security threats, human-related threats, technological threats and environmental threats. These threats have the potential to cause harm to hospital systems and severely compromise the integrity and confidentiality of ePHI. Because of the growing number of security threats, many hospitals, both private and public, are struggling to secure ePHI due to a lack of robust data security plans, systems and security control measures. The purpose of this study was to explore the security of electronic personal health information in a public hospital in South Africa. The study was underpinned by the interpretivism paradigm with qualitative data collected through semi-structured interviews with purposively selected IT technicians, network controllers', administrative clerks and records management clerks, and triangulated with document and system analysis. Audio-recorded interviews were transcribed verbatim. Data was coded and analysed using ATLAS.ti, version 8 software, to generate themes and codes within the data, from which findings were derived. The key results revealed that the public hospital is witnessing a deluge of sophisticated cyber threats such as worm viruses, Trojan horses and shortcut viruses. This is compounded by technological threats such as power and system failure, network connection failure, obsolete computers and operating systems, and outdated hospital systems. However, defensive security measures such as data encryption, windows firewall, antivirus software and security audit log system exist in the public hospital for securing and protecting ePHI against threats and breaches. The study recommended the need to implement Intrusion Protection System (IPS), and constantly update the Windows firewall and antivirus program to protect hospital computers and networks against newly released viruses and other malicious codes. In addition to the use of password and username to control access to ePHI in the public hospital, the study recommends that the hospital should put in place authentication mechanisms such as biometric system and Radio Frequency Identification (RFID) system restrict access to ePHI, as well as to upgrade hospital computers and the Patient Administration and Billing

(PAAB) System. In the absence of security policy, there is a need for the hospital to put in place a clear written security policy aimed at protecting ePHI. The study concluded that healthcare organisations should upgrade the security of their information systems to protect ePHI stored in databases against unauthorised access, malicious codes and other cyber-attacks.

KEY TERMS: Privacy, confidentiality, personal information, security, ePHI, digital health technologies, public hospital, disclosure of information, security threats and South Africa.

DECLARATION

Name: Kabelo Given Chuma

Student number: 50119869

Degree: Master of Information Science

Security of Electronic Personal Health Information in a public hospital in South Africa

I, Kabelo Given Chuma, declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____
(KG Chuma)

_____
Date

DEDICATION

This dissertation is dedicated to my family, including my late father, **Willy Motsamai Chuma,** for his support and presence in my life (September 1956 – November 1999) may his soul rest in peace; my dear mother, **Victoria Mosebodi Chuma,** who has always been my source of inspiration and gave me strength and support when I had thoughts of giving up; my siblings, **Brian Mosa Chuma**, **Karabo Gold Chuma**, **Kamogelo Gaven Chuma, Moses Kgomotso Chuma, Annah Mapula Chuma** and **Mathapelo Sharon Chuma**. I hope this study inspires them to never give up on their dreams. Not forgetting my dearest wife, **Molebogeng Vanessa Rakau,** and lovely daughter, **Tshimologo Chuma,** whose unyielding love, tolerance and encouragement have enriched my soul and inspired me to pursue and complete my research study. All of you have been my best cheerleaders.

Most of all to the one who gives me a
chance to live and gives me strength
and faith to overcome difficulties
"Our heavenly father"

ACKNOWLEDGEMENT

"For I the Lord your God, will hold your right hand, saying to you, fear not, I will help you" (Isaiah 41:13)

Above all, I am most grateful to the ALMIGHTY God for giving me strength, wisdom and encouragement to complete this dissertation. Without His blessings, this dissertation would not have been completed successfully.

First and foremost, my heartiest gratitude is directed to my supervisor, Professor Mpho Ngoepe, for his patience, unwavering support, tireless guidance, continuous supervision, advice and insight throughout the course of this study. He was the backbone of this research project by giving valuable suggestions and constructive criticism which gave the study a life. This dissertation could not have been completed without his unconditional support and motivation. I would like to express my humble gratitude to him for his willingness to spare me his time and to guide me to complete this dissertation within the allotted time. Secondly, I am indebted to the editor of my dissertation, Mrs Letitia Greenberg, for providing a good manuscript with meticulous work.

I am forever thankful to my fellow colleagues of the Department of Information Science at the University of South Africa for their timely support in this endeavour. My special appreciation and thanks goes to the CEO of the selected hospital, for providing me with all the required facilities. A special thanks to Mrs Phenyo Seloane, for assisting me to conduct this study in the public hospital. The financial support of the University of South Africa is gratefully acknowledged. My sincerely appreciation goes to all the staff members of the selected hospital who willingly participated in this study and spared their valuable time to provide useful information and share their invaluable insights and experience with me.

I would also like to say a heartfelt thank you to my dear, loving mother and my siblings for their endless love, prayers and constant moral support throughout my research endeavour. I'm deeply indebted to my wife for always believing in me, encouraging me in all my pursuits and inspiring me to follow my dreams. A special thank you to my one and only princess, for being my stress reliever.

Last, but not least, I cordially thank everyone who contributed in this dissertation; it would not have been possible to complete this dissertation without their continuous support and encouragement. I dedicate this milestone to them.

May the good lord in his infinite mercy bless you all!!!

Kabelo G Chuma

January, 2020

TABLE OF CONTENTS

ABSTRACT I
DECLARATION III
DEDICATION IV
ACKNOWLEDGEMENT V
LIST OF FIGURES XII
LIST OF TABLES XIII
LIST OF ACRONYMS AND ABBREVIATIONS XIV
CHAPTER ONE 1
INTRODUCTION 1
1.1 Introduction 1
1.2 Background information on healthcare data security issues 2
1.2.1 State of healthcare data security in South Africa 6
1.3 Problem statement 9
1.4 Research purpose and objectives 10
1.5 Conceptual framework 10
1.6 Significance of the study 12
1.7 Scope and delimitations of the study 13
1.8 Definition of keywords 13
1.8.1 Confidentiality 14
1.8.2 Disclosure of information 14
1.8.3 Personal information 14
1.8.4 Privacy 15
1.8.5 Security 15
1.9 Literature review 15
1.10 Research methodology 16
1.11 Structure of the study 16
1.12 Summary 18
CHAPTER TWO 19
LITERATURE REVIEW ON THE SECURITY OF EPHI 19
2.1 Introduction 19

2.2 Policy and regulatory framework governing the security of ePHI 20
2.2.1 Legislation and regulations 20
2.2.2 Security standards 25
2.2.3 Security policies and procedures for ePHI 27
2.3 Security threats to ePHI 29
2.3.1 Cyber security threats 29
2.3.2 Human-related threats 34
2.3.3 Environmental threats 37
2.3.4 Technological threats 37
2.4 Security control measures to protect ePHI 38
2.4.1 Administrative security controls 39
2.4.2 Physical security controls 40
2.4.3 Technical security controls 40
2.5 Privacy issues associated with ePHI 41
2.5.1 Unauthorised access and data sharing 41
2.5.2 Data storage and use 42
2.5.3 Data ownership 43
2.5.4 User profiles 43
2.5.5 Misuse of electronic health data 43
2.5.6 User authentication 43
2.5.7 Confidentiality and integrity 44
2.6 Strategies to enhance the security of ePHI in healthcare organisations 44
2.7 Summary 45
CHAPTER THREE 47
RESEARCH METHODOLOGY 47
3.1 Introduction 47
3.2 Research paradigm 48
3.3 Research approach 50
3.4 Research design 52
3.5 Population 53
3.6 Sampling method 54

3.7 Data collection method(s) 54
3.8 Data analysis method(s) 55
3.9 Trustworthiness 56
3.10 Ethical considerations 57
3.11 Evaluation of the research methodology 58
3.12 Summary 58
CHAPTER FOUR 60
DATA ANALYSIS AND PRESENTATION OF FINDINGS 60
4.1 Introduction 60
4.2 Data analysis 60
4.3 Demographic profile of the participants 61
4.4 Presentation of the research findings 62
4.4.1 Policy and regulatory framework governing the security of ePHI in a public hospital 64
4.4.2 Security threats to ePHI in a public hospital 69
4.4.3 Security control measures undertaken by the public hospital to protect ePHI 72
4.4.4 Privacy issues associated with ePHI in the public hospital 77
4.4.5 Recommended strategies for enhancing the security of ePHI in the public hospital 78
4.5 Summary 80
CHAPTER FIVE 82
DISCUSSION AND INTEPRETATION OF FINDINGS 82
5.1 Introduction 82
5.2 Discussion and interpretation of findings 82
5.2.1 Demographic profile of participants 83
5.2.2 Policy and regulatory framework governing the security of ePHI in a public hospital 83
5.2.3 Security threats to ePHI in a public hospital 86
5.2.4 Security control used by the public hospital to protect ePHI 88
5.2.5 Privacy issues associated with ePHI in a public hospital 92
5.2.6 Recommended strategies for enhancing the security of ePHI in a public hospital 93
5.3 Summary 95
CHAPTER SIX 96
SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS 96

6.1 Introduction 96
6.2 Summary of the findings 97
6.2.1 Policy and regulatory framework governing the security of ePHI 97
6.2.2 Security threats to ePHI in a public hospital 98
6.2.3 Security control measures to protect ePHI 98
6.2.4 Privacy issues associated with ePHI 99
6.2.5 Recommended strategies for enhancing the security of ePHI 99
6.3 Conclusions 99
6.3.1 Policy and regulatory framework governing the security of ePHI 100
6.3.2 Security threats to ePHI 100
6.3.3 Security control measures 101
6.3.4 Privacy issues associated with ePHI 101
6.3.5 Recommended strategies for enhancing the security of ePHI 101
6.4 Recommendations 102
6.4.1 Policy and regulatory framework governing the security of ePHI 102
6.4.2 Security threats to ePHI 103
6.4.3 Security control measures to protect ePHI 103
6.4.4 Privacy issues associated with ePHI 104
6.5 Suggestions for future research 105
6.6 Implications of the study 106
6.7 Final conclusion 107
REFERENCES 109

APPENDIXES

Appendix A: Data protection laws and regulations 139
Appendix B: ISO Standards 142
Appendix C: Interview guide 143
Appendix D: Unisa ethical clearance letter 149
Appendix E: Letter seeking permission to conduct research in a public hospital 152
Appendix F: Letter of permission to conduct research in a public hospital 154
Appendix G: Informed consent 155
Appendix H: Declined application letter 156
Appendix I: Declined application letter 157

LIST OF FIGURES

Figure 1.1: Security framework for ePHI (Researcher 2019) 11
Figure 2.1: Literature review structure 19
Figure 2.2: Themes of security controls (Kruse et al 2017) 39
Figure 3.1: Research methodology map 48
Figure 3.2 Research designs (Creswell 2014) 52

LIST OF TABLES

Table 3.1: Summary of study population 54
Table 4.1: Demographic information of the participants 61
Table 4.2: Themes, categories and sub-categories 63

LIST OF ACRONYMS AND ABBREVIATIONS

APT	Advanced Persistent Threats
CCD	Continuity of Care Document
CCR	Continuity of Care Record
CDS	Clinical Decision Support
DDoS	Distributed Denial of Service
ECT	Electronic Communication and Transaction Act
EHR	Electronic Health Records
EMR	Electronic Medical Records
EPHI	Electronic Personal Health Information
EPR	Electronic Patient's Records
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
HITRUST	Health Information Trust Alliance
HPCSA	Health Professions Council of South Africa
IDS	Intrusion Detection System
IPS	Intrusion Protection System
ICT	Information Communication Technology
ISO	International Standards Organisation
MIS	Minimum Security Standards
NHA	National Health Act
NHS	National Health Service
NIST	National Institute of Standards and Technology
OECD	Organisation for Co-operation and Development
PAIA	Promotion of Access to Information Act
PAJA	Promotion of Administrative Justice Act
POPI	Protection of Personal Information Act
RFID	Radio Frequency Identification
WHO	World Health Organisation

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The security of electronic personal health information (ePHI) has become a global concern to the healthcare in the last few years. As increasing amounts of personal health information (PHI) is being collected through a plethora of electronic modalities by healthcare organisations, ensuring the security of such information has become a major issue globally (Beck, Gill & De Lay 2016:320). The security of ePHI is important for healthcare organisations that use computers and systems to avoid any interference or compromise might lead to ethical, privacy and legal issues. Gritzalis and Lambrinoudakis (2004:730) caution that the health information security is an important issue, especially when dealing with sensitive information, particularly in the healthcare settings where the nature of information is critical and confidential.

EPHI is known to be sensitive and volatile in nature. Given the sensitive nature of ePHI, the healthcare industry continues to be a prime target for security threats and breaches. Healthcare organisations across the globe suffer from security threats, breaches and risks. Abouzakhar (2013:10) states that hacking attacks, malware, disasters and insider attacks are the most common threats to healthcare data. Such security threats severely compromise the integrity, availability and confidentiality of patients' health data. In view of the sensitive nature of healthcare data and the mounting information security risks, it is critical for healthcare providers to have a robust and reliable information security service in place. This study explores the security of ePHI in a public hospital in South Africa. It should be noted that the public hospital opted to remain anonymous; hence, it is not identified by a name. Throughout the study, it is referred to as a public hospital. Similar studies carried out elsewhere by Makhubela (2017) in the mining industry and Chigada (2015:124) in the banking sector also did not identify the context of the study in order to protect the interest of the site of study. This chapter puts things into perspective by introducing the study. The following section presents the background information on healthcare data security issues.

1.2 Background information on healthcare data security issues

The healthcare industry has been adopting digital health technologies to enhance the healthcare systems and facilitate the delivery of appropriate health services to the populace. With the introduction of digital health technologies and digitisation of health data, an increasing number of hospitals and peripheral health facilities across the globe are transitioning from a predominantly paper-based practice environment to an electronic or paper-light environment (Zeng 2016:114). As a result, this transition has greatly improved the efficiency and productivity of hospitals, clinics and health administration services, while making patients' data more accessible, allowing for global health networking and increasing access to and quality of healthcare. Overall, these changes have led to a significant increase in the collection, use and sharing of patient health data across organisational boundaries. More and more hospitals are embracing new technologies with the ultimate aim of providing better and safer care. Sittig and Singh (2011:1284) state that the integration of information technology into the healthcare industry shows the conversion of paper-based patients' health records to electronic patients health records. As a result, this transition has greatly improved the efficiency and productivity of hospitals, clinics and health administration services, while making ePHI more accessible, allowing for global health networking and increasing access to and quality of healthcare. The adoption of digital health technologies including Health Information System (HIS), mHealth and telehealth are currently being used by many healthcare organisations to execute digital transformation, increase administration efficiency and widening access to electronic health information.

In a healthcare environment, many healthcare facilities from different countries have developed HIS to capture and manage ePHI. According to Mair, May and Murray (2009:123), HIS allow for the acquisition, storage, transmission, and display of administrative or clinical activities related to patients, such as electronic health records (EHRs). Health systems such as EHR, personal health record (PHR), clinical decision support (CDS), tele-health and telemedicine, have added value to healthcare facilities by presenting new modes for capturing, processing and exchanging ePHI. Viswanath and Kreuter (2007:133) state that HIS have revolutionised the way ePHI is gathered, disseminated and used by healthcare providers**,** patients, citizens and mass media. These systems

connect patients to physicians, clinicians, nurses, hospitals and clinics, and ensure that ePHI is available anytime and anywhere, permitting healthcare practitioners to access patient information.

Many studies have been conducted to understand the implementation of HIS in healthcare organisations. The adoption of HIS in the health industry has increased rapidly to enhance the efficiency of healthcare. Indeed, many developed countries have successfully implemented HIS collection and dissemination of PHI in a digital format (Rozenblum, Jang, Zimlichman, Salzberg, Buckeridge, Forster & Bates 2011:288). Charles, Gabriel and Searcy (2015:10) revealed that 97% of hospitals in the United States of America (USA) have implemented EHR systems. In the United Kingdom (UK), Australia and the Netherlands the use of EHR in the healthcare industry has increased rapidly to enhance the efficiency of healthcare. In Germany, the use of EHRs by general practitioners (GPs) has increased by more than 90% (Singh & Muthuswamy 2013:1535). In Finland, all public sector healthcare providers and almost all private healthcare organisations have adopted EHR (Luna, Emily, Matthew, Sullivan & Clemens 2016:9). Bergkvist (2015:89) reports that New Zealand has achieved an EHR adoption rate of 97% and a large number of public healthcare facilities in Korea have fully adopted EHRs. Mugo and Nzuki (2014:59) state that physicians in Sweden make use of EHR.

In Africa, many countries are starting to embrace health technologies to improve the quality of healthcare service delivery. Litho (2010:66) states that developing countries have demonstrated an increasing application of e-health systems for healthcare delivery.In Africa, although fewer countries have implemented EHR systems for capturing and processing electronic health information, there has been a slow adoption of integrated EHR systems in other countries. African countries like Uganda, Tanzania, and Ethiopia have successfully integrated EHR systems (Scott & Mars, 2015:25-37). Most countries like Nigeria, Rwanda, Kenya, Ghana, sub-Saharan and Zimbabwe are facing a plethora of challenges such lack of ICT Infrastructure, financial constraints and poor internet connectivity and limited bandwidth to implement and adopt EHR systems. These challenges hinder the successful implementation of EHR systems in most African countries (Khalifehsoltani & Gerami, 2010; Akanbi, Ocheke, Agaba, Daniyam, Agaba, Okeke & Ukoli, 2012:01). In South Africa, private hospitals have successfully implemented EHR systems, however, majority of public hospital still make use of paper-based record system (O'Mahony,

Wright, Yogeswaran & Govere 2014:06). Different countries have adopted different approaches for the use of healthcare systems.

The increasing adoption and use of these technologies added value to healthcare facilities by presenting new modes of processing, capturing, storing and exchanging patients' data and information, such as medical history, results of laboratory test, diagnoses, billing and others related hospital procedures while allowing better efficiency in the exchange of health information. Catwell and Sheik (2009:12) argue that these technologies allow for improved delivery of and access to healthcare advice for remote regions, reduced travelling costs and improved communication between patients and healthcare providers. Despite the increasingly widespread adoption and the successful implementation of these technologies in healthcare, the issue of privacy and security remain an ongoing concern for patients. Herman, Flite and Bond (2012:712) caution that the number of concerns about privacy and security of PHI is increasing day-to-day. The fact that the concerns about the sensitive information security and privacy are increasing every year, it can be ascribed to technology-related trends in the healthcare, such as clinician mobility and wireless networking, blockchain, portal technology, cloud computing, Internet of Things (IoT) and social media.

A study conducted by Rothstein and Talbott (2007:38) estimated 25 million annual compelled authorisations for the disclosure of health records in the United States. In Denmark, Germany and New Zealand, respondents also expressed their security concerns with regard to patients' health data (Zurita & Nøhr 2007:6). Chhanabhai and Holt (2007:8) state that 202 (73.3%) of the participants expressed some compatibility issues and concerns about the privacy and the security of patients' data. Papoutsi, Reed, Marston, Lewis, Majeeds and Bell (2015:86) report that 130 (79%) of the participants in the UK expressed higher concerns regarding the security of patient information as a result of this information travelling over the internet. Furthermore, a survey in the USA revealed that 112 (75%) patients are concerned about health websites sharing their information without their permission (Raman 2007:301).

Several studies have reported a number of cases regarding security breaches in healthcare. For example, in 2012, Verizon's data breach investigation reported that its forensic investigation and

security division had compiled data from 47,000 reported security incidents and found 621 confirmed data breaches (Verizon 2013:10). In 2013, Kaiser Permanente (one of the largest non-profit healthcare providers in the USA) notified its 49,000 patients that their health information had been compromised due to theft of an unencrypted USB flash drive containing patient records (McCann 2013:180). Furthermore, a study on patient privacy and data security showed that 80 (94%) of the studied hospitals had at least one security breach in the past two years (Ponemon Institute 2012). In most cases, insider attacks are the common threat experienced.

In view of the foregoing information, it becomes clear that ensuring the security and privacy of ePHI is critical, because the disclosure of ePHI could result in social stigma, loss of employment and denial of medical benefits (Lee, Chang, Lin & Wang 2013:112). In addition, unauthorised access to billing information may result in patients suffering financial losses from illegal transfers of money. Mei, Dawei, Guoliang and Yuan (2009:832–843) confirm that protecting private and important information (such as credit card details or patients' medical records) from attackers or malicious insiders is of critical importance. Due to the sensitivity of health information captured in the HIS, the security and privacy are the most critical aspects in the healthcare environment. Samadbeik, Gorzin, Khoshkam and Roudbari (2015:40) emphasised that ensuring the privacy and security of patients' health information is the key element in building the trust required to realise the potential benefits of electronic health information exchange.

The increasing use of health technologies have caused ePHI to be exposed to a variety of new threats and risks. Such threats come from numerous sources such as hostile governments, terrorist groups, disgruntled employees, and malicious attacks. Ponemon Institute (2017:112) recently reported that nearly 90% of healthcare organisations across the world are suffering from ever-growing number of threats and breaches. According to Snell (2015), hacking and cyber threats such as malware, ransomware and phishing are among the leading cause of breaches in healthcare organisations. A series of recent studies revealed that security threats such as malicious codes, ransomware, phishing, hackers, distributed denial-of-services, Trojan horses and viruses are prevalent in healthcare facilities (Capelão & Barbosa 2018:24; Partala et al 2013:113; Zarei & Sadoughi 2016:85). Other security threats may be related to human threats, technological threats, and natural and environmental threats (Narayana, Ahmad & Ismael 2010). Because of the growing

number of security threats, many hospitals and healthcare facilities are struggling to secure the protection of ePHI due to a lack of robust data security plans, systems and security control measures (HIPAA 2015:111).

The implications of these threats can have a negative impact on the hospital integrity, which may cause destruction of the entire hospital database. In view of this, there is a need for healthcare organisations to carefully and cautiously explore and understand the major threats associated with patient health data, so that appropriate security control measures are properly devised against any security risk. To avoid these emerging threats to ePHI, healthcare providers (hospitals, clinics, outpatient care centres, and specialised care centres) need to develop security defence mechanisms, policies and standards to address identified risk associated with ePHI. HIPAA (2015:112) states that healthcare organisations should strongly invest in security systems and operational best practices to ensure that they are prepared to endure and defend themselves against these security threats. Furthermore, Mehraeen (2012:28) concludes that the implementation and continuous enhancement of security measures and policies are necessary to overcome weaknesses in different dimensions of information security.

1.2.1 State of healthcare data security in South Africa

According to Mugo and Nzuki (2014:52), developing countries are now realising that they have to embrace ICTs to deal with the problem of access, quality and costs of healthcare. South African healthcare organisations are continuously adopting ICTs to improve the quality and safety of healthcare with the increasing numbers of South African private and public hospitals that are transitioning from paper-based documentation to EHRs. The Department of Health (South Africa) (2008:60) points out that the South African healthcare industry has acknowledged the potential of information technology systems and have embarked on ICT projects to implement national EHR as part of the national e-Health Strategy. A study conducted by Ethics Institution of South Africa in 2000 indicated that public and private healthcare sectors are showing confidence in the ability of information technology to transform the industry and to improve healthcare services (Landman, Mouton & Nevhutalu 2000:40). However, some hospitals in South Africa are still rooted in traditional manual processes to capture and manage patient records. This is confirmed by the study

conducted by De Villiers (2006:67), which established that some hospitals in South Africa use computerised or digital record-keeping systems and some use both paper-based and electronic systems, while others do not keep records at all.

Seahloli (2016:83) indicates that public and private hospitals in South Africa have partially implemented HIS for the purpose of capturing, storing and managing patients' health data. HIS such as AS400, ClinicomTM, Unicare, DHIS, Delta 9TM, Medicom, Meditech, Nootroclic, PAAB, PADS, SAP and SORIAN have been implemented by hospitals in different provinces. Mars and Seebregts (2008) advocate the view that these systems cater for entry and maintenance of demographic information of a patient, printing of labels and tracking of patient visits to the hospital. However, the majority of hospitals in South Africa are still using a paper-based filing system (O'Mahony et al 2015:115). According to the study conducted by Cilliers and Wright (2017:89), the South African NDoH has implemented HIS in their public healthcare sector. Their study revealed that public hospitals in five out of the nine provinces have some form of EHR system operational. In the KwaZulu-Natal province, some hospitals use the Medicom and Meditech systems, while in the Western Cape; a few hospitals use the ClinicomTM systems (Cilliers and Wright 2017:89).

Hospitals in the Limpopo province also use the Unicare and Medicom systems (Ataguba & McIntyre 2012). The Meditech system is used mainly in the Free State; the PAAB system in Gauteng, North West and Mpumalanga; the Delta 9 system in the Eastern Cape and Nootroclin in the Northern Cape. Furthermore, private hospitals (Netcare, Life Healthcare and Mediclinic) are using SAP and AS400 systems (Seahloli 2016:88). These HIS are used by hospitals in both the public and private healthcare sectors; however, they are not integrated with one another due to the lack of bandwidth (Kahn 2011:102). Some hospitals do not have any form of system in use nor do they have internet connectivity. The implementation of different systems from various vendors presents a challenge, as they are built with different underlying database architectures and, therefore, they often fail to communicate and share information among them. Although these systems have been implemented in some areas, the majority of the public hospitals in South Africa still make use of a paper-based record system (Department of Health South Africa 2012).

The implementation of these systems poses a number of challenges to healthcare facilities. Some of the challenges include security issues and privacy concerns, along with the issue of cost-effectiveness in securing databases. The privacy concerns affecting the implementation of electronic health information instead of paper-based filing systems are the risk of security breaches and identity theft, which are not as common in paper-based filing systems. There is a growing body of literature that indicates that the South African public healthcare sector, like those in most developing countries, is burdened with many challenges, such as security and privacy issues.

South Africa has recently become one of the top African countries with the highest number of security threats and breaches, particularly in the health and business sector. According to the study done by Ponemon Institute (2016), the healthcare industry has ranked the highest per capita data breach cost in 2016 amongst other industries in South Africa. In 2015, the average per capita cost of data breaches in South Africa was 1.87 million. The report also states that South Africa and Brazil remain the two countries with the highest percentage of human error data breaches. IT News Africa (2016:12) reports that large numbers of hospitals in South Africa are experiencing high volumes of security threats. Although not much research has been conducted to report security breaches in South African healthcare, it has been reported that South Africa lost approximately R50 billion in 2014 due to cyber-incidents, and that over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (SABC 2017). In 2011, estimates put the financial losses from cyber-attacks at R3.7 billion in direct losses and R6,5 billion in indirect costs (Norton South Africa 2012). These threats have become more widespread, as the number of internet users increases in South Africa.

South African healthcare organisations are faced with an increasing number and size of internal and external security threats and breaches that risk PHI falling into the wrong hands. In South Africa, there have been many scandals in which patients' electronic health records were leaked and breached. One example of the security breach to personal privacy, was the leaking of electronic patient records of the late former Minister of Health, Dr Manto Tshabalala-Msimang, to the press August 2007, resulting in an article entitled "Manto: a drunk and a thief". However, the newspaper was sued for divulging health information of the patient (Adesina, Agbele, Februarie, Abidoye & Nyongesa 2011:4). As a result, it is critical for hospitals to implement appropriate security control

measures such as legislation, security standards and security systems, which are essential for securing and protecting ePHI, while satisfying healthcare compliance mandates. According to the Health Professions Council of South Africa (HPCSA) (2008), healthcare providers are responsible for the safeguarding of their patients' health information. Therefore, stringent precautions should be taken to assure the security of the data storage unit used to store patient information, and if necessary, healthcare practitioners should take appropriate authoritative professional advice on how to keep information secure before connecting to a network.

In South Africa, insufficient attention has been paid to the security of ePHI within healthcare organisations, however many previous studies focused on the implementation of EHRs, the impact of EHRs. Therefore, in order to bridge the current research gap, this study aims to fill this gap in knowledge by exploring the security of ePHI in a public hospital in South Africa. The findings of this study can be used to improve the security of ePHI.

1.3 Problem statement

The overarching problem that prompted this study is that the vast majority of South African hospitals are experiencing a dramatic rise in the number and size of security threats and breaches such as the manipulation and theft of personal health information of patients. According to Mchunu (2012:03), there are a number of security limitations and breaches that threaten the integrity, confidentiality and availability of patients' health data in the South African healthcare information systems. Cybercriminals have been reported to be stealing patients' health data in South African hospitals and clinics. Stolen health data are then used to fill "false patient claims to insurers and government agencies that provide healthcare services" (Republic of South Africa 2010:2). In April 2010, thousands of electronic patient files of the Frere Hospital in the Eastern Cape (South Africa) were found to be freely available on the internet (Stone 2010:14). These files contained sensitive PHI such as patient names, certificate number, account number, medical record number, electronic mail addresses and home addresses. IT News Africa (2016:45) reports that a number of hospitals in South Africa have been targeted by malware, phishing and ransomware in 2016, causing a massive financial loss and putting patients at risk. These emerging threats have the capacity to corrupt the integrity of healthcare systems and compromise the availability and confidentiality of

ePHI. Although the implications of these security threats are clear, the causes are not understood. As a result, solutions to these threats remain unsought and unfound; hence, there is a need to explore the security of ePHI in a public hospital in South Africa.

1.4 Research purpose and objectives

The purpose of this study was to explore the security of electronic personal health information in a public hospital in South Africa, with a view to recommend the control measures to safeguard ePHI. The specific objectives were to:

- analyse existing policy and regulatory framework governing the security of ePHI in a public hospital in South Africa
- assess the security threats to ePHI in a public hospital in South Africa
- examine security control measures undertaken by the public hospital to protect ePHI
- assess privacy issues associated with ePHI in a public hospital in South Africa
- recommend strategies to enhance the security of ePHI in a public hospital in South Africa.

1.5 Conceptual framework

Miles, Huberman and Saldana (2013:20) define conceptual framework as a "textual or visual representation of the interactions between the concepts, variables and or assumptions upon which the research is based". The conceptual framework is used by researchers when existing theories are not applicable or sufficient to create a firm structure for the study (Akintoye 2015). According to Ngulube (2020:29) and Nieswiadomy (2012:29), there are various ways in which a conceptual framework can be formulated for a research study. This includes (i) putting together various concepts from different theories, (ii) aspects of a theory, (iii) incorporating aspects of a theory, (iv) integrating all the concepts from more than one theory, and (v) combining concepts from the extant literature. Based on a review of the literature, the researcher developed a conceptual framework that supports the security fundamental to ePHI in healthcare organisations. The researcher found critical concepts from the literature that can be used towards the development of a conceptual framework. These concepts include: (i) policy and regulatory framework, (ii) security control

measures, (iii) security threats, and (iv) privacy issues. Figure 1.1 illustrates the interaction among these concepts to convey the security of ePHI

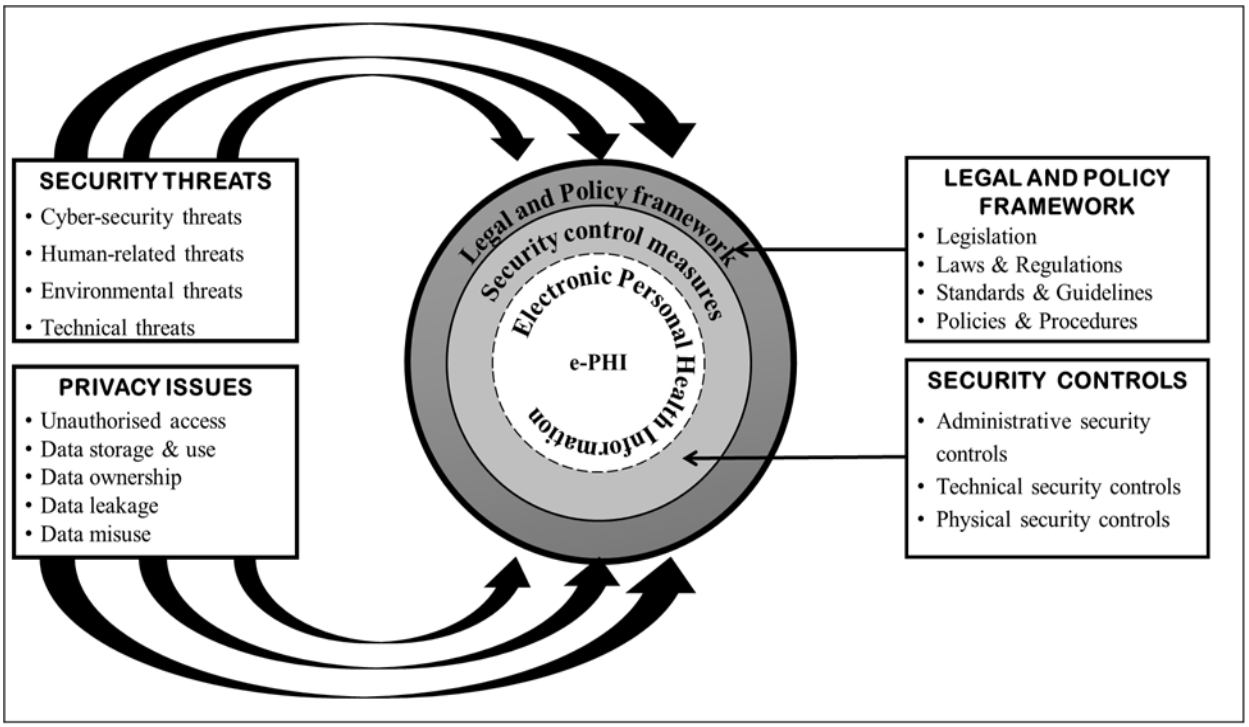


Figure 1.1: Security framework for ePHI (Researcher 2019)

The main objective of this study is to consider the security required for ePHI; therefore, the focus is on the relationship between legislation and regulations, security threats, security control measures and privacy issues. The conceptual framework presented in this study is designed to provide a structured approach to researching factors that may be important in understanding the security of ePHI. Security control measures form a crucial role in achieving the security and protection of ePHI. An understanding of how these concepts interplay can help to ensure the security of ePHI.

In a hospital, documented bureaucratic policies and procedures, legislation and regulations and International Security Standards need to take place to guide internal employees on how to protect ePHI from potential security threats. These dimensions serve as important forms of internal control. Security threats can be mitigated by corresponding security controls, such as administrative, physical and technical controls. If security control measures are not fully or

correctly implemented, it may result in security threats to ePHI not being mitigated. Therefore, there is a need for healthcare providers and stakeholders to take all the necessary precautions and measures to ensure appropriate security of healthcare patient information. Doing so, this should provide adequate overall risk mitigation against various security threats.

1.6 Significance of the study

This study is significant to provide insights into the security of ePHI in a public hospital in South Africa. The outcome of the study is expected to provide evidence of data upon which relevant policies can be formulated and the defensive mechanisms that can be deployed to mitigate the security threats. Ngoepe, Mokoena and Ngulube (2010:39) support the importance of this study when they stress the need for records management professionals and IT personnel to maintain privacy and security of data are issues that cannot be left unattended. Healthcare organisations face many ethical issues in the conduct of their business such as security, confidentiality and privacy of information (Ngulube 2000:161). Therefore, there is a need to address these issues, hence the researcher embarked on this study. Although a considerable number of studies have been conducted about ethics and security of patients' health records in public hospitals (Luthuli & Kalusopa 2017; Marutha 2018; & Katuu 2015), only a few studies dealt directly with the security of ePHI in public hospitals. For this reason, this study attempts to fill the gap by exploring the security of ePHI in a public hospital in South Africa.

This study will contribute to national efforts in the modification and formulation of security policies and laws that effectively address the security of ePHI in the South African healthcare sector. This study hopes to establish an enhanced understanding of the security of ePHI in a public hospital. Most importantly, it is hoped that this study will enlighten hospital managers and stakeholders to be aware of the security threats to ePHI. Studies have shown that security threats have a significant impact on organisational and financial performance (Abouzakhar 2013:10), and that healthcare organisations have experienced a host of security threats that negatively impact on patient health data. Therefore, the results from this study might assist hospital managers and stakeholders in identifying best practices to minimise security threats and to plan for the future protection of ePHI in a public hospital. This study will raise awareness of policy makers and

implementers regarding appropriate measures to be taken in the eradication of the security threats faced by the public hospital. The recommendations in this study can be used to improve the security of ePHI in the public hospital. Overall, this study is expected to contribute to the existing body of knowledge in the area of health information security, to bridge the gaps in the identified literature and to provide new directions for further studies that can be explored related to this research topic.

1.7 Scope and delimitations of the study

The present study is explorative in nature and focused mainly on the security of ePHI in a public hospital in South Africa. This study was carried out in one public hospital in South Africa and other hospitals were not taken into account. This is because the researcher sought to explore the security of ePHI at a fine-grained level of detail that cannot be achieved through multiple hospitals. Furthermore, the researcher chose to focus on one hospital in order to investigate the topic in far more detail than might be possible if he was trying to deal with a large number of study participants with the aim of 'averaging'. This study will not give a general conclusion on the security of ePHI in other hospitals that are geographically spread out. However, the findings from this study could help broaden understanding of the fundamental security and protection of ePHI. The study was delimited to the current employees working in the hospital and ex-employees, clients, partners or other types of stakeholders were excluded from the study. This study was delimited by parameters such as population and methodological design. Population samples for this study were drawn from IT personnel, administrative workers and records management staff. However, medical professionals (doctors and nurses) and patients were excluded from the study, based on the assumption that they are not knowledgeable about the security and protection of ePHI. Methodologically, the study used a qualitative research approach and a single case study design. Finally, the results of this study may not give general conclusion to other hospitals, which are distributed throughout the country.

1.8 Definition of keywords

This study uses a number of terms or concepts that readers may be familiar or unfamiliar with. This section provides the working definitions of key terms used in the context of the present study. All definitions are supported by authoritative sources considered reliable for the purpose of the present study and intended to clarify terms for the intended audiences and decrease ambiguity. The keywords identified for this study include:

1.8.1 Confidentiality

Confidentiality can be defined differently depending on the context in which you use the term. In the simplest sense, confidentiality means respecting and protecting someone else's information and that it is not supposed to be disclosed to unintended people or entities. Confidentiality in the context of healthcare refers to the obligation of professionals who have access to patient records or communication to hold that information confidential (McWay 2010:174). Confidentiality is about the patient's information.

1.8.2 Disclosure of information

Disclosure of information is the act of revealing or exposing proprietary or sensitive information that has been kept as a secret. In healthcare, the term 'disclosure of information' means communicating confidential patient information to others in accordance with legal guidelines (Yarmohammadian, Raeisi, Tavakoli & Nansa 2010:140).

1.8.3 Personal information

The term personal information encompasses a broad range of information associated with an individual. According to M.Prem (2016:44), personal information includes information about a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, and criminal behaviour or biometric information. Personal information can be regarded as recorded information about an identifiable individual other than contact information. In the healthcare setting, personal information is a category of sensitive

information that is associated with a patient, including the fingerprints, biometric data, names and surname, telephone number, email address or social security number (HIPAA 2015:99).

1.8.4 Privacy

The term privacy has been defined in different ways, but a widely agreed definition remains elusive. It is a difficult term to define because it means different things to different people in different contexts at different times. In general sense, privacy is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others (HIPAA 2015:72). From the perspective of health, privacy specifically refers to the right of patients to determine when, how, and to what extent their health information is shared with others (Andriole & Khorasani 2010:397). Privacy is about patients.

1.8.5 Security

According to Davidson (2005:80), the term "security" may have different meanings for different people given the time, place and context. In a general sense, security may be considered as the protection of information, objects, people or assets to avoid any disruption or harm. Within the context of healthcare, security refers directly to protection, and specifically to the means used to protect the privacy of personal health information and support professional institutions in holding that information in confidence (HHS 2014). According to Patil and Seshadri (2014:181), security is described as "physical and technological measures that can be used to protect healthcare data from unauthorised disclosure or illegal access of any restricted data."

1.9 Literature review

The review of literature exposes the researcher to available literature and offers new ideas, perspectives and approaches to the topic. Cheung and Waldeck (2016:10) define a literature review as "an evaluative report of information in the literature related to the selected area of study". The review should describe, summarise, evaluate and clarify the literature. The purpose of a literature review is to convey to the reader what knowledge and ideas have been established on a chosen

topic and what their strengths and weaknesses are. The literature review must be guided by the research objectives and research questions (Cheung & Waldeck 2016:10). Through literature review, a researcher acquires what has already been covered in the chosen research area and is enabled to problematise the study's implications for future research. The review of related literature for this study is arranged into the following five themes in line with the research objectives of the study: (a) policy and regulatory framework governing the security of ePHI; (b) security threats to ePHI; (c) security control measures to safeguard ePHI; (d) privacy issues associated with ePHI and (e) strategies to improve the security of ePHI in healthcare organisations**.** Chapter Two of this study provides a detailed literature review on these five themes.

1.10 Research methodology

Research methodology is the general research strategy that outlines the way in which research is to be undertaken and, among other things, also identifies the methods to be used in it. These methods define the means or modes of data collection or, sometimes, how a specific result is to be calculated (Howell 2013:330). Shensul (2012:103) asserts that research methodology is the strategy that researchers use to ensure that work can be critiqued, repeated and adapted. According to Creswell (2014a), there are three main research approaches, namely the quantitative approach, the qualitative approach and the mixed methods approach. For the purpose of this study, the qualitative approach was adopted as it best suited for this case study to obtain a comprehensive and in-depth knowledge about the security of ePHI in a public hospital. Accordingly, data were collected through structured interviews with purposively IT staff, administrative staff, records management staff and system security staff, and triangulated with document and system analysis. A thematic analysis of the data was used to identify, analyse and report patterns within the data. The data were transcribed and categorised into themes. A detailed exposition of the research methodology is provided in chapter three of this study.

1.11 Structure of the study

This dissertation comprises six chapters. The content of the six chapters is discussed below.

Chapter One: Introduction and background

This chapter discussed the introduction and background to the study, as well as the research problem, the aim of the study, the research questions, the scope and delimitation, the preliminary literature review, conceptual framework and a summary of the methodology. The definitions of keywords and an outline of the study were also presented.

Chapter Two: Literature review

This chapter provides a detailed review of existing empirical and theoretical literature covering the security of ePHI. The literature review of this study is divided into the following four main sections (in this sequence): policy and regulatory framework that governs the security ePHI, security threats to ePHI, security control measures to safeguard ePHI and privacy-related issues associated with ePHI. Gaps in literature were identified and the ways in which these are addressed by the present study are discussed.

Chapter Three: Research methodology

This chapter provides the research design and methodology of the study; explain the way in which the study will be conducted; and outline the research approach, design, population and sampling, data collection methods and procedures, trustworthiness, ethical considerations, data analysis and data presentation.

Chapter Four: Data analysis and presentation of findings

This chapter focuses on the analysis and presentation of the findings from the semi-structured interviews, document analysis and system analysis.

Chapter Five: Discussion and interpretation of findings

This chapter discusses and interprets the study findings presented in Chapter Four. The discussion is supported by extant literature and the theories underpinning the study.

Chapter Six: Summary of findings, conclusions and recommendations

This chapter concludes with a detailed summary of findings, conclusions drawn from the results of the study, and recommendations that arose from the study. Areas for future research are also

provided in this chapter. Appendices will be included as part of the study, which includes an interview schedule, ethical clearance, research permit and authorisation letters from the hospitals approached.

1.12 Summary

This first chapter puts the research into perspective by providing an introduction to and background of the study. The chapter provided the problem statement, research objectives, research questions, significance of the study and the study site. Theoretical key concepts used in the study were identified and defined. This chapter also provided a summary of methodology and research design used in the study. The significance of the study was highlighted was been discussed in this chapter and a brief outline of the sequence of chapters was outlined. The next chapter discusses the literature review.

CHAPTER TWO

LITERATURE REVIEW ON THE SECURITY OF EPHI

2.1 Introduction

The previous chapter set the scene by providing the introduction and background to the study, problem statement, research purpose and objectives, research questions, significance of the study, scope and delimitation of the study, conceptual framework, research methodology, as well as the definition of key terms. This chapter presents the literature review based on the different perspectives of the scholars and researchers in correspondence with the ePHI privacy and security field. Literature review is a critical summary of existing knowledge on a topic of interest, often prepared in order for the research problem to be placed in context (Polit & Beck 2008:757). According to Abbas (2015:46), "literature review captures published and unpublished work from secondary sources and draws attention to important variables, as determined in previous studies that are related to the research problem being investigated and significant findings in the area of investigation". A literature review allows a researcher to present the viewpoints of other researchers and build on existing knowledge (Onwuegbuzie, Leech & Collins 2012:28). Figure 2.1 presents the themes and sub-themes to be covered in the literature review.

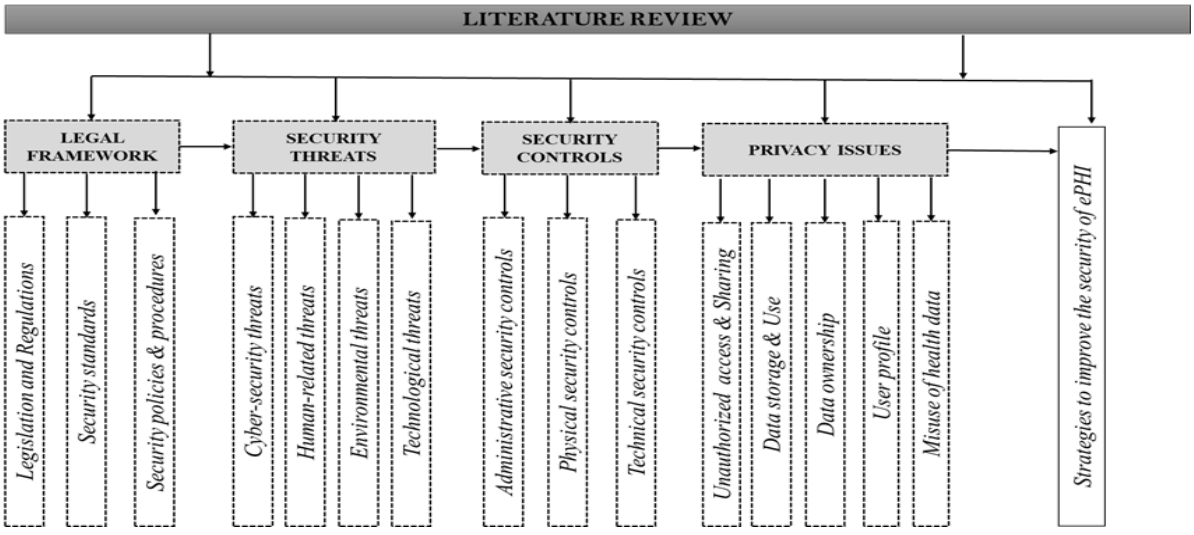


Figure 2.1: Literature review structure

2.2 Policy and regulatory framework governing the security of ePHI

The conceptual framework developed in this study provides a systematic way of understanding the security of ePHI through policy and legislative framework. A policy and regulatory framework is critical to healthcare governance. The policy and regulatory framework comprises a summary of significant policies, standards and legislation to secure ePHI in healthcare organisations. In this chapter, relevant key legislation, security standards and policies pertaining to the security of ePHI in healthcare organisations are reviewed. Some specific literature has been assessed in order to find out what work was done by research professionals, scholars and organisations in this area. Hospitals and other healthcare organisations are subject to health legislation and regulations, standards and policies regulated by the country concerned. As the number of security threats and data breaches increases, the need for data protection legislation and regulations has become increasingly important in healthcare industry.

Legislative and regulatory frameworks are an essential tool for improving healthcare governance at the country level. Without legislation and regulations, authority is not set, the privacy and confidentially of patient health information are compromised and patient health information in the electronic platform is exposed to other threats and risks. According to Magnusson (2017:385), legislative framework refers to "legislation that sets out structures for governance and accountability or other processes for guiding the decisions and actions taken by government or the executive". In the health environment, legislative framework consists of comprehensive laws and acts, standards and guidelines, policies and procedures that govern the protection and security of ePHI. Considering the importance of security and privacy, many countries have adopted different regulation frameworks and standards focusing on achieving data integrity, confidentiality and availability of health ePHI.

2.2.1 Legislation and regulations

Hospitals and other healthcare organisations are subject to healthcare legislation regulated by the country concerned. Legislation is an essential part of any healthcare organisations to ensure effective protection of ePHI. These healthcare legislation and regulations provide the foundation

for strong and resilient healthcare systems. In all countries, the operation of healthcare systems and uses of ePHI within healthcare organisations are governed by a complexity of legislation and regulations, which set out the government's requirements to be met by healthcare organisations to ensure the security of ePHI. Asija and Nallusamy (2014:58) state that healthcare regulatory requirements are statutory laws that establish licensing or regulatory agencies or boards to generate rules that regulate medical practice. In the healthcare industry, cyber security threats and data breaches are severe and can pose significant security risks to ePHI. To deal with these security issues, various laws and regulations are made. The implementation of legislative and regulatory frameworks in healthcare organisations can help to accomplish a secure environment. In this regard, it is crucial for healthcare organisations to comply with healthcare laws and regulations. Asija and Nallusamy (2014:58) elaborate that failure to comply with healthcare laws and regulations may constitute civil (intentional disclosure of ePHI is a non-compliance) and criminal (knowing misuse of unique health identifiers and for knowingly and impermissibly obtaining or disclosing individually identifiable health information) penalties such as a fine or imprisonment. These health laws and regulations address some of the issues and protect patients' privacy and security by specifying penalties to individuals breaching the legal barriers. Compliance with legislation, laws and regulations can help healthcare organisations to continue to improve the quality of care.

A number of countries around the world have developed legislation and regulations to regulate data protection. As an example, the US Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy and security of US patient data (HIPAA 2013). HIPAA governs with the US legislation for healthcare privacy by defining rules to ensure that PHI that is stored by healthcare providers would not be disclosed or used in a way that would violate patient privacy. It also permits the disclosure of ePHI needed for patient care and other important purposes (OCR 2008). Asija and Nallusamy (2014:59) aver that HIPAA security rule has established national standards for the security of individuals' ePHI. New Zealand is one of the countries that have privacy legislation to guarantee data security and privacy. The 1993, the Privacy Act of New Zealand was one of the most comprehensive privacy acts outside the European Union (NZPA 1993). Furthermore, Australia has a set of laws and legislation concerning privacy. New South Wales Health Records and Information Privacy Act, 2002 (NSW HRIPA), is the most recent

legislation passed in Australia that relates to health information privacy (New South Wales Government 2002).

Makulilo (2012:178) presents arguments to emphasise that African countries such as Angola, Burkina Faso, Tunisia, Morocco and Senegal have adopted privacy legislation: however, countries in sub-Saharan Africa, such as Uganda, Rwanda and Tanzania, are still in the process of implementing privacy laws. Other countries such as Ghana, Ivory Coast, Kenya and Mali have Bills on similar law pending before their legislative bodies (Makulilo 2012:178). A study conducted by Farzandipour, Ahmady, Sadoghi and Karimi (2008:149) note that countries such as Malaysia and Iran have few legislation and regulations concerning disclosure of patients' health information.

The South African government has established a number of legislation to govern the security and protection of personal information. Healthcare organisations in South Africa are controlled by a considerable number of legislation and regulations to protect sensitive information, such as the Protection of Personal Information Act of 2013 (POPI Act); Promotion of Access to Information Act of 2000 (PAIA), National Health Act of 2003 (NH Act); Promotion of Administrative Justice Act of 2000 (PAJA); Electronic, Communication and Transaction Act of 2002 (ECT Act); National Archives of South Africa Act of 1996. This legislation and regulations prohibit the disclosure or misuse of sensitive information about private individuals.

The POPI Act is among the major national policy document that shapes the way that electronic healthcare information is being accessed and used in hospitals and other healthcare facilities (De Bruyn 2014). The POPI Act affects organisations that deal with the most sensitive personal information such as names, addresses, health information, and employment history. The POPI Act regulates the processing of personal information by both public and private institutions, notes that health information is considered a special kind of personal information and has to be managed effectively (South Africa 2013:32). The POPI Act is aimed at safeguarding personal information. This aims to align South African legislation with international data protection standards. In order to protect the personal information of patients, South African hospitals are required by law to adopt and be guided by the POPI Act. The POPI Act has committed to the objective of regulating the

manner in which personal information may be processed by establishing conditions, in harmony with international security standards that prescribe the minimum threshold requirements for the lawful processing of personal information.

The PAIA Act, which facilitates access to records, notes that access to health records should be given to ensure that the disclosure does not cause serious harm to the physical or mental health, or well-being of the requester (South Africa 2000:30). The Act aimed to provide access to information held by public and private organisations such as healthcare facilities. According to Marutha and Ngulube (2010:10), the purpose of the PAIA Act is to ensure the protection of people's rights. For instance, patients in the public health sector have the right of access to information to their medical records.

The NH Act requires that personal information concerning patients which has been collected by hospitals should be treated as confidential. According to Lungile, Luthuli and Kalusopa (2017:03), the NH Act guides institutions on how health departments should be governed in both public and private hospitals. The aim of the Act is to build a national healthcare system that governs both public and private health services; therefore, ensuring that everyone has access to equal health services. Chapters 14, 15 and 16 of the NH Act are pertinent with confidentiality. With regard to the position of personal data and privacy protection in South Africa, Chapter 2 of the NH Act has particular relevance. Confidentiality-related provisions are set out in section 14, and section 15, through 1797, provides for access to health records and their protection. Chapter 16 of the Act describes how patients' records may be disclosed by hospital workers for any legitimate purpose. These sections effectively strengthen the ethical principles of confidentiality into a statutory requirement (Oosthuizen & Verschoor 2008).

The Constitution of the Republic of South Africa Act, No. 108 of 1996 (Constitution), sets out South Africa's values and the rights of the people. This Act aimed at protecting the rights of the people inside the country and it explains their obligations. According to Marutha and Ngulube (2010:07), section 195 of the Constitution focuses on the basic values and principles governing public administration. This section emphasises effective, economical and efficient use of resources, the provision of timely, accessible and accurate information. It also stipulates that public

administration must be accountable. The Constitution plays a major role in South African healthcare organisations. This Act provides laws that protect patients and it also enshrines the rights of patients.

South African healthcare organisations are required to comply with PAJA. According to Marutha (2011:55), PAJA was introduced to bring about a "lawful, reasonable and fair" administrative action and to ensure the proper documentation of these actions in accordance with section 33 of the Constitution. In healthcare organisations, this legislation is aimed at protecting patients from unlawful, unreasonable and procedurally unfair administrative decisions.

The ECT Act has a significant impact on the healthcare sector. The implication of this Act is that all departments are encouraged to implement electronic systems that are characterised by security, integrity and authenticity (PNC 2006:22-23). The ECT Act enables and facilitates electronic communications and transactions in the public interest in South Africa. One of the objects of the ECT Act is to promote e-government services and electronic communications and transactions with public and private bodies, institutions and individuals. The Act also provides the framework within which authentic and reliable records or data messages should be created of such transactions and communications (ECTA 2002). Sections 50 and 51 of the ECT focuses on personal information that has been obtained through electronic transactions. The ECT Act sets out the accepted data protection principles, describing how personal data, as defined in the ECT Act, may be collected, used and processed within organisations.

The National Archives of South Africa Act, No. 43 of 1996, provides the legislative and legal framework for how records management practices in governmental bodies are regulated and makes it clear that institutions dealing with health services must ensure that records relating to health services are created and maintained at that health institution for further service delivery. In South Africa, government departments are under legislative obligations to adopt a systematic and organised approach to the management and the security of health records (Ngoepe 2008:2).

In South Africa, if health data is breached, there are consequences for the healthcare organisation's brand and reputation as well as an associated financial impact, for instance as prescribed by the

POPI Act and PAIA (Evans, Maglaras & Jaicke 2016). Marutha (2018) stresses that non-compliance with legislation leads to poor management of electronic health records, which also causes difficulties for healthcare institutions in their attempt to produce quality data for creating knowledge to support organisational decision-making and problem solving. In terms of the POPI Act (2013), non-compliance with legislation and regulations in South Africa may result in fines, loss of reputation, litigation or other consequences for the healthcare providers. Importantly, such non-compliance may have wider public interest implications in terms of potential substantial harm to healthcare providers. Different countries have different laws for data protection. A list of relevant legislation is shown in Appendix A that relates to the protection of personal data.

2.2.2 Security standards

According to Tofan (2011:128), security standards are regarded as a "set of requirements that a product or a system must achieve". Security standards are useful to provide guidance to healthcare facilities and other custodians of ePHI on how to best protect confidentiality, integrity and availability of such information. Government authorities in different countries are expected to set up security standards and guidelines for the protection of sensitive health information. Security standards and guidelines in the healthcare industry form a fundamental technical basis for healthcare legislation. Different national or international data protection laws and information-sharing Acts cover security standards and guidelines in the healthcare industry.

Vucetic, Uzelac and Gligoric (2011:573) argue that every healthcare organisation, clinic and hospital has its own information system to maintain patient data. Hence, there is a need to provide security standards and guidelines to ensure that ePHI is processed securely and with proper regard for its confidentiality, integrity and availability. A number of security standards and guidelines have been developed in the healthcare industry, through which health information about patients can be transferred and shared among different healthcare systems. The standards include International Standards Organisation (ISO) and Minimum Security Standards (MSS). Healthcare organisations are required to implement the relevant standards to protect sensitive information of patients.

ISO is an international organisation for standardisation that provides a set of international standards, guidelines and characteristics. Dickinson, Fischetti and Heard (2004) state that ISO standards define how health information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between healthcare systems. According Tofan (2011:128), ISO has established a number of standards series and ensures that information and systems are securely protected. The ISO 27000 standards series includes ISO27799, ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005 and ISO 27006, whereas the SP800 standard series include standards such as SP800-12, SP800-45, SP800-50, SP800-63 and SP80095. These standards and guidelines have been specifically retained by ISO for information security issues in various organisations, including health organisations. According to the NHS CFH (2010:56), healthcare institutions and facilities should ensure that they are compliant or working towards compliance with security standards to show that information security is being considered seriously and that effective steps to information security are in place. This also gives confidence to interested parties.

The MSS are a set of security standards for the minimum information security measures that should be undertaken by institutions and organisations to protect any sensitive personal information. The MSS are standards that deal with information security within an organisation. In South Africa, the MSS are aimed at protecting sensitive information of individuals. South African healthcare organisations are required by the law to implement the MSS to protect the PHI of patients. The MSS provide minimum security standards for handling information that is collected by hospitals in South Africa. Hospital systems that handle PHI of patients must comply with all the MSS standards.

In South Africa, ISO and the MSS are adopted in the healthcare sector to manage and protect sensitive and valuable information about patients' and healthcare providers. Coleman's (2010) study points out that ISO 27799 was adopted by the South African public healthcare sector in 2008. This standard was published by the ISO technical committee, TC215, which is responsible for the health informatics (Coleman 2010). The ISO 27799 is based on ISO 27001 and ISO 27002 which ensure that an appropriate level of information security management is in place. In the security standard ISO 27001, risks, vulnerabilities, and threats to organisational strategies are the main

objectives (Alebrahim, Hatebur, Fassbender, Goeke & Côté 2015). This standard provides healthcare organisations with a blueprint for implementing effective security controls and policies. The overall objective of ISO 27799 is to provide healthcare organisations with fundamental guidelines to protect PHI.

These standards support the implementation of security control measures in healthcare organisations and they serve as a tool for protecting PHI. By implementing these standards, healthcare organisations and other providers of health information will be able to ensure that a minimum requisite level of security is appropriate for an organisation's circumstances. This is to ensure that confidentiality, integrity and availability (CIA) of PHI both in printed and digital format are maintained at all times (Coleman 2010). These standards emphasise the need for protecting patients' privacy and confidentiality in healthcare organisations. The adoption of these standards by healthcare organisations will enable the safe adoption of new health technologies in the delivery of healthcare services. Secure and privacy-protective health information sharing can significantly improve healthcare outcomes. As a result of implementing these security standards, healthcare organisations across the globe can expect to see the number and severity of their security threats and risks reduced, allowing resources to be redeployed to productive activities. Appendix B describes the general security standards for protecting data.

2.2.3 Security policies and procedures for ePHI

The term 'policy' is used in the management literature in two related but distinct ways. In general, policy refers to an organisation's grand plan or strategy which defines its overall goals and objectives. More narrowly viewed, policy refers to specific statements that define desirable and unacceptable management practices. This second definition most clearly conveys the level of concern in this study. A security policy is a formal document that defines responsibilities, acceptable use and security practices for healthcare organisations to protect sensitive PHI. According to Knapp and Ferrante (2012:79), security policies are ideal when the policy assists employees in understanding how an employee's behaviour can affect an organisation with respect to protecting information and computer systems. The security policy involves three aspects:

prevention of unauthorised access into the system, controlling the input and output of the system, and monitoring the healthcare information systems (Lin & Clark 1994:2).

The security policy should include the availability, integrity, and confidentiality of information stored and transmitted between IT systems and end-users (Knapp & Ferrante 2012:79). In the healthcare environment, security policies and procedures are important technical mechanisms to protect ePHI against various threats, risks and breaches. Hospital managers are expected to develop a sound security policy that addresses all the requirements to protect people, processes, data and technology. Vucetic et al (2011:573) assert that healthcare organisations require strict security policies and procedures governing the use of physical media and portable devices to prevent theft or loss of patients' health data. Healthcare staff are expected to comply with and keep up to date with numerous security policies covering the security of ePHI. Adherence to these security policies and procedures will help them to keep their networks secure, maintain secure transmission of ePHI data and protect the confidential information of their patients. The absence of security policy in healthcare organisations can lead to harmful security results such as loss of confidentiality, integrity or availability of ePHI.

In the same vein, Keen, Calinescu, Paige and Rooksby (2013:243) advocate the view that the key to the success of exploiting healthcare data are the information policies that dictate how to access and use this information. Because of the sensitive nature of health information that is being digitally transmitted and accessed, healthcare data policies and procedures can be protective and defensive of that information (Pasquale 2013:772; Terry 2013:90). According to Cucoranu et al. (2013:89), a lack of security policy and procedures in the hospital for securing electronic health information can cause a number of conflicts such as unauthorised access, destruction, use, modification, or disclosure of sensitive health information. Healthcare organisations and all individuals within hospitals are required to comply with, and give due consideration to, the data protection policies and procedures that apply to their daily work, because failure to appropriately comply with policies and procedures can have serious consequences. According to ROC (2009:45), non-compliance or non-adherence with data protection policies and procedures is a significant problem, which involves both civil money and criminal penalties.

2.3 Security threats to ePHI

In the context of the conceptual framework discussed above, we note that perhaps the most vulnerable threats significantly exposed to ePHI are cyber-security threats, human-related threats, environmental threats and technical threats. Before addressing the security threats to ePHI, it is important to understand the concept 'threats'. Brauch (2011:106) defines a threat as "an action that takes advantage of security weaknesses in a system and has a negative impact on it". Threats can originate from three primary sources: humans, technologies and nature (Duncan, Creese & Goldsmith 2012:862). The vast majority of healthcare organisations are frequently facing an increased number of security threats causing different types of damages that lead to significant financial losses, economic harm and damaged reputations.

As health organisations are more conducive to cyber-threats, it is important to explore the main threats and attacks that these organisations suffer. A number of studies have identified security threats in the healthcare area (Stoneburner, Goguen & Feringa 2002; Partala et al 2013; Narayana et al. 2010; KPMG 2017). According to these studies, the most widespread security threats to electronic health information are cyber security threats, human-related threats, natural disasters, and technical threats. The effects of these security threats to ePHI vary considerably, some affect the confidentiality of patients' data while others affect the availability of healthcare systems. These security threats are explained below with respect to their related cases.

2.3.1 Cyber security threats

The term "cyber threat" can be understood as any malicious act that attempts to disrupt or gain unauthorised access to data, systems, digital networks or digital services. Anderson et al (2012) define cyber threats as "those actors or adversaries exhibiting the strategic behaviour and capability to exploit cyberspace in order to harm life, information, operations, the environment and/or property". Cyber threats are typically composed of a combination of threats such as advanced persistent threats (APT), phishing, pharming, spamming, spoofing, Trojan horses, ransomware, wiper attacks, malware attacks, spyware and adware, viruses, eavesdropping rogue software and malvertising.

These security threats have the capability to manipulate typical hospital patients and their information for illegal gain. The healthcare industry faces profound cyber security threats. Elaborating further on this, Jalali and Kaiser (2018:10059) affirm that cyber-security threats are a growing threat to the healthcare industry in general and hospitals in particular. According to KPMG (2017), Ponemon Institute (2016:10) and Wanyonyi, Rodrigues, Abeka and Ogara (2017:120) malware attacks, ransomware attacks, phishing attacks, Distributed Denial-of-Services (DDoS), eavesdropping, spyware and social engineering are the most concerning cyber threats in the healthcare industry. Such threats represent conditions with a potential to cause damage/harm to the healthcare system and manipulate typical health patients and their personal information for illegal gain. In the same vein, Eling and Schnell (2016) explain that cyber threats arise from the use of IT and can damage the integrity, availability, or confidentiality of patients' health data. Consequently, these threats are discussed as follows:

2.3.1.1 Malware threats

Malware represents one of the key threats to healthcare organisations. This security threat has become the leading cause of healthcare data breaches in healthcare organisations. Milošević, (2013:01) defines malware as "a malicious software program used or programmed by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems". It can appear in the form of codes, scripts, active content, and other software. Different types of malware are commonly described as viruses, worms, Trojan horses, backdoors, keystroke loggers, rootkits or spyware and other malicious programs. Avancha, Baxi and Kotz (2012:3) avow that ePHI stored in the database of the healthcare organisations is vulnerable to malware such as viruses, Trojans and worms. These threats have the ability to destroy or disrupt ePHI captured in the system. According to Abouzakhar (2013:73), these external threats can compromise the integrity, confidentiality and availability of a healthcare service provider's information assets. Cluley (2010:56) postulates that malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. Malware threats have the potential to damage the effectiveness or deterioration the performance of healthcare systems. In the same vein, Partala et al (2013:248) mention that malwares have the ability to infect and propagate to the whole hospital

server, which can cause unavailability and disruption. Whereas, changing and updating of software configuration of patient monitoring servers make system configuration unstable, resulting in system malfunctioning and communication interruption, malware threats may lead to serious privacy issues such as loss of reputation, identity theft and reduced patient safety.

2.3.1.2 Ransomware attacks

Ransomware has become one of the fastest growing major threats in the healthcare industry. Spence, Paul and Coustasse (2017:124) emphasise that the rate of ransomware incidents has been growing in the healthcare industry. In the same vein, Wright, Aaron and Bates (2016:1115) declare that ransomware is one of the major cyber threats, has increased dramatically in all countries, leading to a massive loss of patient data or requiring redemption of payment to restore data. Ransomware is one of the most expensive cyber threats that can affect healthcare organisations.

According to Bridges (2008:20), ransomware refers to a type of malware used by attackers that first encrypts files and then attempts to extort money in return for the key to unlock the files by demanding a "ransom". Ransomware is a form of malevolent software, or "malware," that typically encrypts or deletes data stored on computer networks, trapping the data and making it unavailable and unusable (Cadwlader & Taft 2017). Hackers routinely use the variant of ransomware to access the system through a hospital server, encrypt and block hospital users from accessing their health data files on their healthcare systems or server. Gagneja (2017:05) points out that hackers make use of this malicious software to make hundreds of millions of pounds. Variants of ransomware such as Locky or Samas infected individual and business computers in healthcare facilities and hospitals around the world (Sittig & Singh 2016:628). To avoid data theft and undue extortion of ransomware, individuals and organisations need robust network security platform.

2.3.1.3 Phishing attacks

Phishing is another growing threat in the healthcare industry. This strategy is an attempt to "fish" for sensitive health information of patients. Grazioli and Jarvenpa (2013:22) define phishing as

"an internet scam technique used to obtain credit card numbers, account numbers, passwords and other confidential information, often is the first stage of identity theft". According to Zahoor, Ud-din and Sunami (2016:27), phishing is an attack in which an attempt is made by an attacker to obtain sensitive information of users such as usernames, passwords, credit card details, and so on by pretending to be a reliable body in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging in which users are asked to click on a link usually to secure their accounts (Zahoor et al 2016:27)**.**

The healthcare industry is targeted extensively by phishers who frequently gain access to healthcare data stored in email accounts. Phishing attacks on healthcare organisations are implemented by hackers with the intention of gaining direct access to ePHI, or to incur significant financial gain. According to the HIPAA (2013), 91% of cyber-attacks in the healthcare industry come from phishing emails. Hackers send phishing emails to a healthcare employee along with a seemingly legitimate reason for revealing their login credentials. Doing so will give the hackers access to an email account and the ePHI of patients in those emails. These phishing attacks result in the hospital losing access to their system and compromising the care for the patients. These attacks potentially lead to leakage of private patient data (Solander, Forman & Glasser (2016:55). Protecting against these attacks will be the next challenge.

2.3.1.4 Distributed Denial of Service

Today, Distributed Denial of Service (DDoS) is recognised as one of the greatest security threats facing healthcare organisations across the world. Elleithy, Cheng and Sideleau (2005:71) define DDoS as "any type of attack on a networking structure to disable a server from servicing its clients". Attacks range from sending millions of requests to a server in an attempt to slow it down, flooding a server with large packets of invalid data, to sending requests with an invalid or spoofed IP address. Denial of Service (DoS) attacks pose a serious problem for healthcare organisations**.** According to Chauhan and Prasad (2015:215), DDoS attackers can shut down EHR and email systems, which could prevent providers from accessing or communicating critical patient information. Once the server of the hospital is down, an attacker is able to deter patients or healthcare personnel from accessing critical healthcare assets such as

payroll systems, electronic health record databases, and software-based medical equipment such as magnetic resonance imaging (MRI), electrocardiogram (ECG) and infusion pumps. (US-CERT 2016). DDoS attackers use thousands of different IP addresses to send different types of data packets to the targeted server or network (Chauhan & Prasad 2015:215). DDoS attacks can damage the wireless healthcare application network, and can lead to the loss of the patients' information.

DDoS attacks are increasing in frequency on the healthcare industry. According to Ponemon Institute (2016), a number of healthcare organisations had experienced DDoS attacks, which is the fifth most common crime after malicious code crimes, unauthorised access, spam email and spyware. In 2014, one of the largest children's hospitals in the United State was attacked by DDoS. The hospital's website was unreachable and lost productivity for a one-week period, which resulted in hundreds of thousands of dollars to be spent to mitigate and respond to the attack (Ponemon Institute 2016). Protecting against these attacks requires close coordination with service providers to ensure that critical networks can remain operational under a DDoS onslaught.

2.3.1.5 Eavesdropping

Another growing threat in healthcare security is eavesdropping. According to Pawar and Anuradha (2015:506), eavesdropping is a passive attack, which occurs in the mobile ad hoc network. The main aim of this attack is to find out some secret or confidential information from communication. Eavesdropping is one the most common threat to the patient health data. By patient vital sign snooping, an adversary can easily discover the patient information from communication channels. Moreover, if the adversary has a powerful receiver antenna, then he/she can easily pick up the messages from the network. The captured message may contain the physical location of the patient, allowing an attacker to locate the patient's position and physically harm him/her. In addition, an adversary can also detect the message contents, including message ID, timestamps, source address, destination address and other relevant information. Thus, monitoring and eavesdropping can pose a serious threat to patient privacy (Dimitriou & Loannis 2008).

2.3.1.6 Spyware

Spyware is a common attack vector experienced by healthcare organisations**.** Lee and Kozar (2005:77) define spyware as "malicious programs that install themselves on the computer without the knowledge of the user". They monitor every activity of the user, thereby compromising the privacy of the user. They may capture keystrokes of the user and send them to a third party and in this way, potentially exposing usernames and passwords. Eventually this may compromise confidentiality and privacy of ePHI. They may also install unwanted advertising programs called adware. Spyware may automatically be downloaded from websites. Some free or pirated software may contain spyware. Others come as an attachment to the email as spam (Pankomera & Van Greunen 2017:45). Spyware can lead to identity theft, loss of data, financial losses and economic harm, and it can also reduce patient confidence in online safety.

2.3.1.7 Social engineering

Engebretson (2011:78) defines social engineering as "one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherent to every organisation." The foundation of an attack is to persuade the forfeiture of information that is confidential and then exploit an individual or an organisation. In this threat, the attacker may masquerade as a genuine administrator to gain access to healthcare systems and compromise privacy and confidentiality of patients. Such a person may even alter the contents of an electronic health record, which may affect the integrity of health records. Authorised users in the hospital can also disclose patient data to concerned parties such as a health insurance company for unethical personal intends.

2.3.2 Human-related threats

Security threats to ePHI are not only caused by malicious external attackers, instead they can be the result of actions by internal employees who ineffective technology or processes. Human threats can be regarded as threats caused by intentional human actions to harm the computer system. According to Duncan et al (2012:862), human threats are those threats caused by people, such as malicious threats consisting of internal (someone has authorised access) or external threats (individuals or organisations working outside the network) looking to harm and disrupt a system.

Braithwaite et al (2007:601) aver that people may pose a serious threat to the integrity of the health data. In healthcare organisations, the most common forms of security incidents caused by human beings are system misconfigurations, poor patch management practices, poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorised hardware and software, access by unauthorised users and lack of knowledge. Human threats can arise from insider threats, hacking and terrorism. These three threats are discussed as follows:

2.3.2.1 Insider threats

Insider threat is a major threat bringing severe damage to the ePHI. According to Williams and Woodward (2015:316) insider threats are issues created by the mistakes or deliberate actions of staff (responding to phishing emails – a social engineering attack to extract login credentials or to launch a malware attack, erroneous security settings, misuse of passwords, losing laptops and sending unencrypted emails). Insiders can negatively affect the confidentiality, integrity, or availability of the organisation's information or information systems. Millar (2011:5) asserts that insider threats are the most difficult to defend against. They can be manifested as poorly trained, malicious, negligent, or terminated employees committing computer abuse, theft, using malicious code, selling information and gaining unauthorised system access.

Alshehri, Mishra and Raj (2014:168) addressed that insiders may obtain credentials from legitimate healthcare providers authorised to access the target ePHI in several ways including: (a) asking for and obtaining credentials from authorised users, (b) using authorised users' unattended logged-in machines, (b) stealing or illegally obtaining credentials from authorised users, (d) stealing devices that contain the credentials of authorised users, and (e) stealing devices or storage containing the ePHI. Healthcare organisations should implement access control mechanisms to mitigate unauthorised access by external users, i.e., outsiders, although it is more challenging to mitigate insider threats as they already have some authority to access ePHI in the system (Alshehri et al 2014:169).

2.3.2.2 Hacking

Hacking has become one of the most significant threats to the national and international healthcare organisations. Williams and Woodward (2015:316) define hacking as unauthorised access to a computer system to gain information or cause disruption. Hacking is one of the common threats to ePHI in the healthcare system. Snell (2015) cautions that hacking has become the leading cause of health data breaches. Hackers are increasingly targeting the healthcare sector because its healthcare systems tend to contain information that is more lucrative. The sensitivity of the healthcare data collected and stored in healthcare databases is vulnerable to hackers and cyber criminals. In healthcare organisations, hackers can access ePHI of patients via a number of routes, including poorly protected passwords, liberal access privileges, or dormant accounts of former employees. They can also email gambits, remote logins to gain unauthorised access to the organisation's financial, administrative and clinical information systems. Avancha et al (2012:3) claim that hackers can create a code with malicious content to steal the patients' information and take control of the organisation's network. Hackers will continue to take advantage of lax security to steal ePHI, deny access to health services or cause intentional harm.

2.3.2.3 Cyberterrorism

Cyberterrorism remains a complex and dynamic global threat in healthcare organisations. Denning (2012:194) defines cyber terrorism as the convergence of terrorism and cyberspace, which means unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimate or coerce a government or its people in the furtherance of political or social objectives. Denning (2000) defines cyber terrorism as: "cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives". Cyber terrorism involves the use of the internet as both enabler and support mechanism. It has the potential of creating a postmodern state of chaos. It uses computer resources to intimidate, harm, or disrupt critical infrastructures such as power grid, transportation, oil and gas, banking and finance, hospital, water, and emergency services. Clem, Galwankar and Buck (2003:275) advocate the view that cyberterrorism has the potential to enable terrorists to attack healthcare facilities with much greater ease and with less moral outrage than would occur with an actual physical attack.

Cyberterrorists can cause harm to systems or alter information using several tactics such as fraud, email floods, viruses, Trojans, worms, spam, phishing, identity theft, spyware, and denial-of-service attacks (Parker 2010:173). Cyberterrorists have the potential to greatly affect the healthcare infrastructure by launching attacks on healthcare systems and disrupting health information about patients. By exploiting vulnerabilities in hospital IT systems, terrorist groups, who traditionally act using physical force, could mount attacks from within safe distances.

2.3.3 Environmental threats

Environmental threats are a big challenge to the healthcare systems and individual health facilities. The impact of environmental threats can seriously disrupt or destroy the functioning of healthcare systems. The most common problem of environmental threats includes natural disasters and man-made disasters. Biswas and Choudhuri (2012:21) define a natural disaster as the outcome when people are affected by natural hazards. The most commonly occurring disasters of nature include: hurricane, earthquake, tsunami, tornado, volcanic eruption, floods and cyclone, wild fire and heat weaves (Rehman 2014:319). Furthermore, Cucoran et al (2013:1) state that this category includes environmental hazards such as power surge, computer room fire, and water leaks from defective sprinklers, heating, ventilation and air-conditioning plumbing, effluent back-flow into sub-floors and natural disasters. These threats have serious financial implications and can also cause disruption of healthcare systems and damage or destroy ePHI. In addition, man-made disasters also pose a serious threat to ePHI stored in the hospital database. Man-made disaster can be regarded as a disaster resulting from man-made hazards, as opposed to natural disasters resulting from natural hazards. Disasters such as water leakages, liquid chemicals and explosions could also harm healthcare systems and cause severe damage to ePHI. These environmental threats can lead to loss or exposure of sensitive health information. In order to avoid natural disasters to affect healthcare institutions, it is necessary to have a disaster management plan.

2.3.4 Technological threats

Technological threats are threats caused by physical and chemical processes on material. Physical processes include the use of physical means to gain entry into restricted areas such as the building,

compound room, or any other designated area like theft or damage of hardware and software. However, chemical processes include hardware and software technologies. It also includes indirect system support equipment like power supplies (Ruf et al 2014). One of the most security risks in relation to computerised health information systems is the danger of technological threats. Technological threats such as power failure of the server, power failure of hospital computers, air-conditioning failure, system crushes, network software failure, systems malfunction, down-time monitor support software failure, and medical record software failure are also treated as high-risk to ePHI captured in the healthcare system (Vaast 2007:152). Narayana et al (2010:203) argue that technological threats present high-risk threats to hospital systems. These threats may have serious implications for healthcare organisations in general and healthcare service providers in particular.

2.4 Security control measures to protect ePHI

The conceptual framework addressed a number of security control measures that must be considered by the healthcare organisations to avoid, detect or minimise security risks and threats to ePHI in the healthcare system. According to Purcell (2007), security controls are measures taken to safeguard an information system from the attacks against the confidentiality, integrity, and availability of the information system. According to Ives (2014:53), there are three pillars to securing ePHI as outlined by HIPAA which include: (a) administrative security controls; (b) physical security controls; and (c) technical security controls. According to HIPAA (2015), healthcare organisations are required to implement appropriate security measures to ensure the confidentiality, integrity, and security of ePHI. They are useful to prevent the risk of loss, unauthorised access, misuse, or destruction of electronic health information about patients (Kim, McGraw, Mamo & Ohno-Machado 2013:72). Figure 2.2 illustrates these security controls.

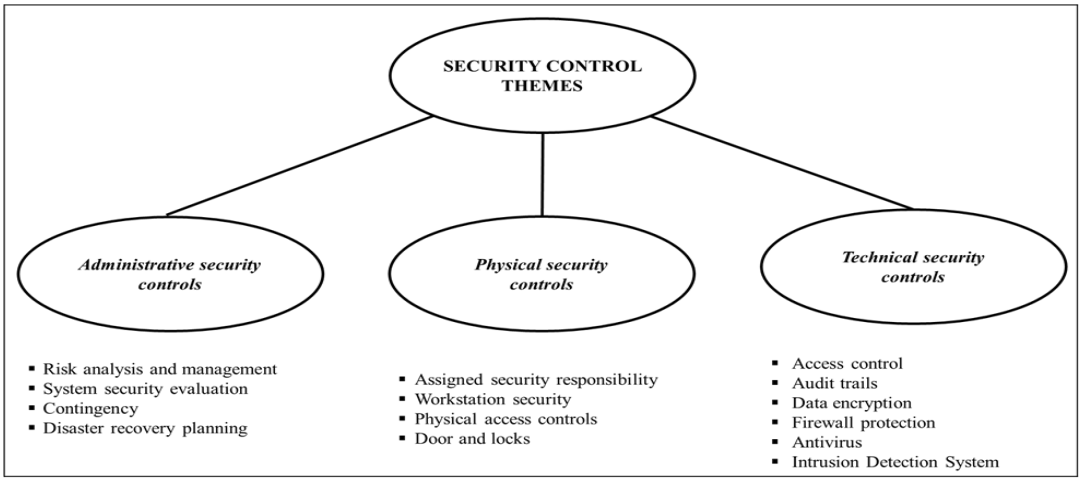


Figure 2.2: Themes of security controls (Kruse et al 2017)

2.4.1 Administrative security controls

According to Yau (2014:2), administrative security controls are primarily procedures and policies which were put in place to define and guide employee actions in dealing with the organisations' sensitive information. Similarly, Kruse, Smith and Vanderlinden (2017:127) state that technical security controls typically take the form of policies, practices, and procedures in the facility to regularly check for vulnerabilities and continually improve the security posture of the healthcare organisation. Administrative security controls consist of approved written policies, procedures, standards and guidelines. They inform people how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations from the government, corporate policy, hiring policy, password policy and disciplinary policy are regarded as administrative security controls (Salkind & Kristin 2007:5).

Andriole (2014:1216) states that administrative security controls include requirements for documenting departmental security policies; training staff on these policies; developing rules and procedures for assigning access to ePHI; maintaining audit trails of all system logs by user identification, activity, and date and time of access; enforcing policies for storage and retention of electronic data and backup of all systems; adhering to specific methods for incident reporting and resolution of security issues; and clearly documenting accountability, sanctions, and disciplinary actions for violation of policies and procedures and implementing a security training and

awareness program for all members of the work force. Examples of administrative controls include staff training, monthly review of user activities and policy enforcement.

2.4.2 Physical security controls

Physical security controls are measures, policies, and procedures to physically protect the Covered Components' Systems and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorised intrusion (HIPAA 2013). The purpose of this security control is similar to limiting access to only authorised parties. According to Cooper and Collman (2005:102), physical security controls include policies, procedures and measures to control physical access to information assets such as computer sites, servers, networks and buildings. According to the study by Andriole (2014:1216), physical security controls include device isolation, allowing direct physical access to authorised personnel only, methods for backing up data and maintaining copies, emergency contingency protocols, and proper device disposal. Other examples of physical security controls within the healthcare organisation include door and locks, heating and air conditioning, smoke and fire alarms, and suppression systems and fencing (Wanyonyi et al 2017:48). These controls are useful to monitor and control the health environment of the hospital and computing facilities within the hospital.

2.4.3 Technical security controls

According to Bhaskar and Ahson (2008:112), technical security controls also known as logical controls, refer to restriction of access to system. Technical security controls typically consist of hardware and software features provided in a healthcare system to ensure the integrity and security of ePHI. Healthcare organisations are expected to implement and develop technical security measures to evade security threats and risks associate with technology. Failure of such security measures may disrupt business continuity and diminish operating efficiency. Technical security controls include authentication controls to verify that a person is authorised to access the ePHI, hardware and software audit controls, ePHI integrity controls and encrypting, and to decrypt data during transmission and storage. According to Cooper and Collman (2005:103) and Lemke (2013:26), technical security controls include the various defensive mechanisms typically

associated with information security such as access control systems, biometrics, password, Audi trail, antivirus, encryption, decryption, firewalls, authentication measures, Intrusion Detection System (IDS), Frequently Identification (RFID), Secure Sockets Layer to evade security threats and assuring health information integrity. These controls remain consistently used defensive security measures for assuring health information integrity. Network intrusion detection systems, access control lists, virtual private networks, tokens for user access, audit logs and public/private key infrastructure are also examples of technical security control (Wanyonyi et al 2017:49). These controls use software and data to monitor and control access to patients' information captured in the hospital system.

2.5 Privacy issues associated with ePHI

The conceptual framework addressed a number of privacy issues in healthcare organisations posed by ePHI. Privacy issues derive from multidisciplinary fields such as computer science, bioinformatics, social sciences and medical science. Healthcare applications (mHealth, telehealth, Dock Health, and eHealth) are being developed while patients have put other applications into use, therefore users and researchers are also starting to raise privacy issues (Ramli, Zakaria & Sumari 2010:745). Privacy is one of the most challenging issues faced by healthcare organisations. Al Ameen, Liu and Kwak (2012:99) state that privacy issues arise from many reasons. It may be personal belief, social and cultural environment and other general public/private causes. Meingast, Roosta and Sastry (2006) mention that privacy implications may arise when integrating from a traditional healthcare system to new health technologies. The transitioning from paper health records to the electronic records has raised a number of privacy-related issues. Understanding the privacy issues is the key challenge with regard to the adoption of new technologies. There are a number of privacy issues that need to be addressed to protect ePHI. The following section addresses the most common privacy issues posed by ePHI in healthcare organisations.

2.5.1 Unauthorised access and data sharing

One of the major concerns in terms of privacy is access and sharing of health data. Nonetheless, unauthorised access to health data remains a problem. Meingast et al (2006) argue that connecting

ePHI to the internet exposes this data to more hostile attacks compared to the paper-based medical records. Since health information about patients is available in electronic format, it opens the door for hackers, cybercriminals and other malicious attackers to breach healthcare systems and steal ePHI for financial gain. The use of electronic healthcare systems allows accessibility to patient health data from different geographical locations and this increases the concern of security, probably violation of patients' privacy. Patients are expected to share personal health information with healthcare organisations. However, they may decline to reveal important information as the disclosure of information may result in social stigma and discrimination (Daglish & Archer 2009:120). Unauthorised access to and sharing of sensitive personal information in healthcare could result in several unwanted usages such as unwarrantable discrimination by employers. Aselton and Affenito (2014:4) argue that sharing and transferring of patients' health data from one hospital to another across different platforms may present problems for patient privacy.

2.5.2 Data storage and use

One of the major concerns in terms of privacy is the storage and use of PHI. Wherever sensitive health data is stored digitally, such as in the cloud, privacy issues become particularly important. Considering the personal nature of such information, the debate of who should be storing the data is also of concern. One major issue related to privacy issues arises from PHI stored in the cloud, is that it can be leaked or hacked by cyberciminals. Healthcare organisations generate a large amount of patient information, driven by record keeping, compliance and regulatory requirements, and patient care.

Owing to the size and speed of health data set, healthcare organisations are faced with many challenges to manage, capture and store such volumes of data. Information can only be used for a specified lawful period of time; however, it does not mention who will decide on this length of time and how to determine the appropriate length (Asghar et al 2017). Ramli et al (2010:743) state that without proper authentication and encryption, unauthorised personnel can take patient data without any difficulty. Every pervasive system should incorporate basic encryption to protect the patient's information.

2.5.3 Data ownership

Data ownership is one of the issues associate with privacy of patients. It is also important when delegation of power to access of patient record is considered. Who will own which data, delegation of authority over data? Furthermore, duties and responsibilities of data ownership should be handled transparently (Huda, Sonehara & Yamada 2009:249).

2.5.4 User profiles

Several entities are involved in the healthcare system like patientd, practitioners, healthcare organisation, trusted third party, pharmacist, and others. Hence, the functional requirements are distinguished from security levels of users (Vucetic et al 2011:572). There is great variability and incompatibility of patient identification systems in healthcare facilities, making it difficult to uniquely identify patients within one facility or between entities. A system of identifying patients between entities must exist for interoperability to occur. Currently, there is no record-to-record matching standard in the industry (Vucetic et al 2011:572).

2.5.5 Misuse of electronic health data

Some of the websites offering EHRs, mostly the ones that offer storage space for free, are not concerned with privacy. They may sell the data to other companies, or advertise on the same page as the content uploaded by the patient (Benhard, Grascher & Neubauer 2008:120). In a multi-speciality environment, security of electronic health records can be challenging. Healthcare organisations must have the ability to segregate any records related to treatment of substance abuse, as treatment of these patients can encompass multiple medical specialities and document types.

2.5.6 User authentication

When any user is trying to access the electronic health record, only authorised users will be able to access the record. Several smart-card-based solutions have been proposed. A biometric-based

system is also in use for ensuring the authorised access of electronic patient records (Yang & Bao 2004:38).

2.5.7 Confidentiality and integrity

Confidentiality is related to the accuracy and reliability of healthcare records and integrity and reliability of physical computer and network systems. Hacking incidents on EHR systems may lead to altering patient data or destruction of clinical systems (Stefankatzenbeisser 2008:112).

2.6 Strategies to enhance the security of ePHI in healthcare organisations

Owing to the numerous threats facing the healthcare industry, there is every need to use effective strategies to improve the security of ePHI in healthcare organisations. Various authors have suggested a number of strategies to improve the security of ePHI. According to Martin, Martin, Hankin, Darzi and Kinross (2017:179), healthcare organisations can improve resilience by maintaining secure and up-to-date backups so that an attack will not result in the permanent loss of healthcare data. According to them, healthcare organisations should develop common security standards. Many general standards exist for cyber security, such as the CIS Critical Controls, NIST 800-53, and ISO27001.30. Other strategies for improving the security of ePHI is that there must be relevant resources, strategic plans toward incidence response must be developed, their staff must be educated, and policies and regulations that guarantee network security must be implemented in order to forestall any attempt of threat.

Gagneja (2017:5) suggests that the healthcare organisations should install defensive mechanisms and detection tools such as Intrusion Detection Systems (IDSs) to detect suspicious activity such as malicious attacks. In another study, Sittig and Singh (2016:682) made a suggestion that monitoring systems should be developed to detect suspicious activity, such as significant increases in network traffic, notification of email messages from unknown sources, or the inclusion of executable as an email attachment. They also state that healthcare institutions should implement methods to encrypt and decrypt ePHI (Sittig & Singh 2016:682). All ePHI stored or transmitted on work systems and slides must be encrypted. Encryption can be used to ensure the security of

the health data and help prevent eavesdropping and skimming. Encryption can be accomplished in hardware as well as in software (Serge 2006:89). Furthermore, a robust and incremental back-up system for health and personal-critical details should be implemented in healthcare organisations. Healthcare organisations should consider storing backed up health information away from the main system if possible.

Researchers like Gritzalis and Lambrinoudakis (2004) suggest that healthcare organisations should regularly upgrade the security of their information systems to protect their databases against unauthorised access. In addition to this, healthcare data policies and procedures that prevent security threats should be enforced in healthcare organisations to prevent and deal with security threats in place. Capelão and Barbosa (2018:3585) propose that healthcare organisations can improve their cyber security by keeping the systems and programs updated and correctly configured, but also to make good management of firewalls and network services to control the means of access to electronic health information. Another strategy for improving the security of ePHI is that healthcare organisations should use systems and security tools such as anti-malware/antivirus software. These security tools should be continuously updated to ensure that healthcare systems receive the best possible protection at any given time. Healthcare organisations should invest in audits and reviews of web applications that could pose ever-evolving security threats. Furthermore, they must be educated about network security and the proper use of devices with access to company networks (Maxfield & Latham 2014:28).

2.7 Summary

This chapter extensively reviewed literature relevant to the security of ePHI in healthcare organisations. The chapter also provided comprehensive and detailed information organised into various sections and subsections. The chapter has been organised in thematic areas which reflected on key research objectives. The literature identified studies that had been conducted on the security and privacy of ePHI in healthcare organisations. The literature review assessed key legislation, ISO standards and security policies that cover the security of ePHI. The literature reviewed discussed a number of security threats most likely to impact negatively on PHI in an electronic format.

The types of threats that exist within the context of health industry were delineated. The literature review addressed the security control measures that can be undertaken by healthcare organisations to ensure the security of ePHI. These include administrative, physical and technical security controls. An understanding of how these security measures relate to one another is important in achieving effective security of ePHI. Finally, literature also indicated a number of privacy-related issues associated with ePHI in healthcare organisations. These include unauthorised access, data storage and use, data ownership, user profile, user authentication and confidentiality and integrity. In an attempt to achieve the objectives of this study, this chapter formed the basis for subsequent chapters to explore different types of security threats to ePHI. The next chapter examines the research methodology employed in investigating the research problems in this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter presented a review of literature to provide the context and further justification of this study, as well as to show where it fits into the existing body of knowledge. The term methodology encompasses two nouns: method and ology, which entails an aspect of knowledge; therefore, methodology is a field of knowledge that involves the commonly professed rule of conduct or proposition of the creation of new knowledge. Jonker and Pennink (2010) define research methodology as "the way researchers conduct research; choose to deal with particular questions (which may result in the definition of a research problem); deal with people or organisations; and establish overall research approaches". Rajasekar, Philominathan and Chimnathambi (2013:110) describe research methodology essentially, as "the procedures by which a researcher goes about his/her work of describing, explaining and predicting phenomena in a research undertaking".

It also provides a description of the assumptions underlying various techniques and procedures used, and explain why certain procedures and techniques are applicable, and others are not. It can also be seen as a way to systematically solve the problems identified in a research. Ngulube (2015:127) indicates that methodology is central to the research process; it is the lens through which a researcher looks at the universe when acquiring knowledge about a social phenomenon and it is able to extract answers by means of the research questions. This chapter covers the research methodology and methods used to explore the security of ePHI in a public hospital. The chapter outlines the research paradigm, research approach, and design of the study, as well as the population, sampling techniques, data collection methods, and instruments used for data analysis. It also addresses the measures to ensure trustworthiness, evaluation of the research methodology and adherence to ethical issues as illustrated in Figure 3.1.

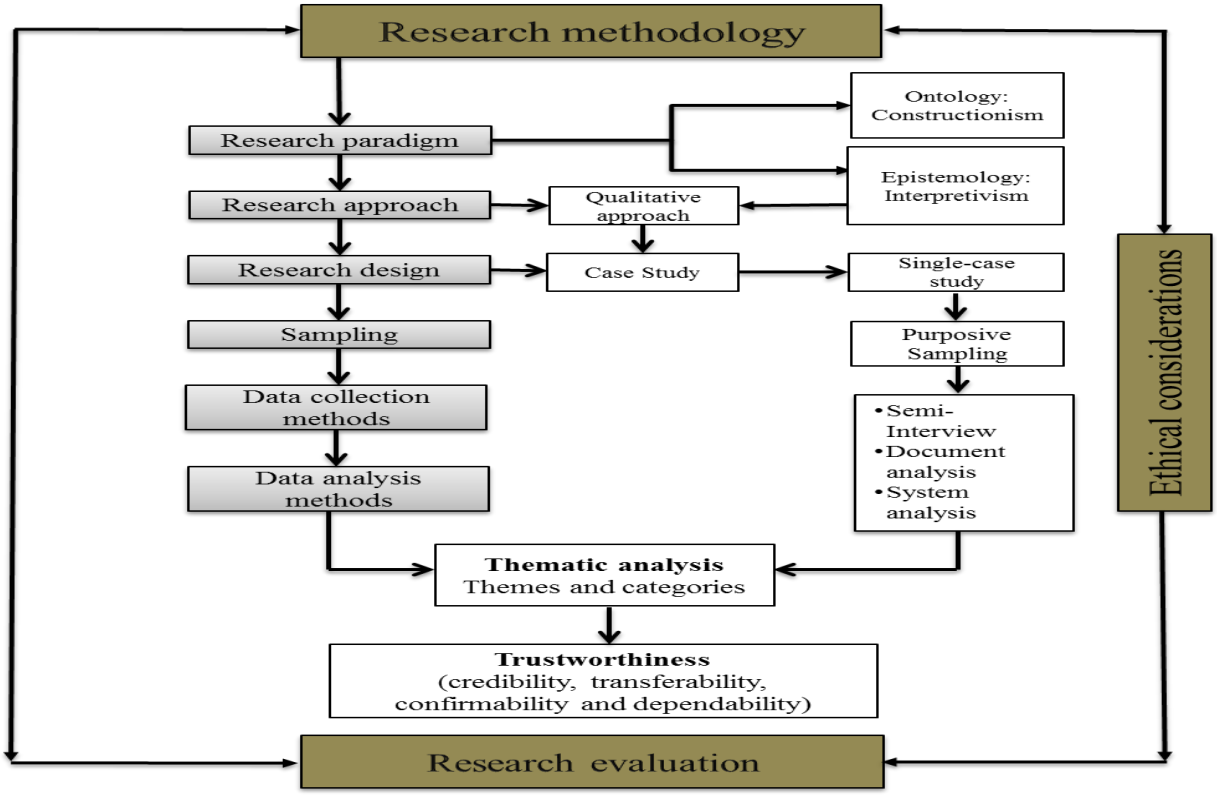


Figure 3.1: Research methodology map

3.2 Research paradigm

Research is a logical and systematic search that is underpinned by various beliefs or schools of thoughts. Some authors, such as Thomas (2010:560), refer to beliefs as paradigms, while others such as Creswell (2009) also refer to them as worldviews. The choice of research paradigms and their compatibility in research methodologies and methods are of paramount importance in any form of research. Bryman (2012:630) defines research paradigm as "a cluster of beliefs and dictates that for scientists in a particular discipline influence what should be studied, how research should be done and how the results should be interpreted". Jonker and Pennink (2010:161), as quoted in Wahyuni (2012:69), explain a research paradigm as a "set of fundamental beliefs and assumptions about how the world is perceived; that forms a thinking framework, which guides the behaviour of the researcher". It shapes how one conducts the study, and it is prudent to adopt a research paradigm at the start of the research process. Therefore, a research paradigm is the totality

of the philosophical framework through which knowledge is produced to improve how things are done (Creswell 2012).

Research paradigms associated with social sciences include the positivism, interpretivism, post-positivist and pragmatism (Creswell 2014; Pickard 2013). These paradigms are discussed in detail as follows:

According to Chilisa and Kawulich (2012:7), a positivism paradigm is a strict worldview that holds that the only way to ascertain truth and objectivity is through the use of scientific methods. Reality is viewed as being objective and knowable. It is an approach inclined towards the natural sciences, as it stipulates that science is the only foundation for true knowledge and that, "the methods, techniques and procedures used in the natural sciences offer the best framework for investigating the social world". This paradigm is consistent with a quantitative methodology. "Such research is value-free and based on precise observation and verifiable measurement" (Chilisa & Kawulich 2012:7).

Chilisa and Kawulich (2012:9) argue that constructivism and interpretivism "are related concepts that address understanding the world as others experience it". This paradigm enables the understanding of how respondents interpret their own experiences within their contexts. Punch (2013) describes interpretivism as "the philosophical positions that people bring meanings to situations, and uses these meanings to understand their world and influence their behaviour". The interpretive paradigm seeks to expose understandings of human behaviour and actions, attitudes that the researcher needs to understand in order to maximise the potential of the research approach. This paradigm is commonly associated with qualitative approaches to data collection and analysis.

Post-positivist paradigm combines both positivist and interpretive paradigms; it accepts that all discoveries are the responsibility of the researcher to demonstrate objectivity during the discovery process (Pickard 2013). Weaver and Olson (2006) point out that post-positivism has emerged in response to the realisation that reality can never be completely known and that an attempt to measure it is limited to human comprehension.

The pragmatism is “a world view arising out of actions, situations and consequences rather than antecedent conditions” (Creswell 2009:10), while according to Teddlie and Tashakkori (2009:7-8), “pragmatism is a deconstructive paradigm that debunks concepts such as truth and reality and focuses instead on what works as the truth regarding the problem under study”. Pragmatic world-view emerges out of deeds, circumstances, and outcomes instead of preceding circumstances, as is the case in scientific method (Creswell 2014). Pragmatism relates to mixed methods approaches in the sense that the researcher draws from both theories, quantitative and qualitative, when they conduct their studies. Scotland (2012) states that different paradigms inherently contain different ontological and epistemological views, and therefore have different assumptions of reality and knowledge underpinning their research approach. Based on the above information, the interpretivism paradigm was adopted as the framework for the present study.

Interpretivism as a paradigm is often associated with other terms like constructionism, naturalism and qualitative approach. It is worth noting the difference between constructionism and subjectivism. However, both are epistemologies, some writers refer to constructionism as ontology (Bryman 2012:210). Interpretivists are concerned with meanings and attempt to understand daily phenomena through the meanings that people assign to them within their social context (Henning, Van Rensburg & Smith 2004). This paradigm enabled the researcher to gain in-depth understanding of the security of ePHI from the point of view of the people working in a public hospital. The interpretive paradigm also provided a context that allowed the researcher to examine what the participants in this study have to say about their experiences in the security of ePHI. Following the above points, the interpretivism paradigm informs the methodologies to be used for this study.

3.3 Research approach

McGregor and Murnane (2010:420) opine that research approaches are methods used to gather and analyse data and present results. There are three dominant research approaches that have been advanced by research scholars Creswell (2014); Leedy and Ormrod (2013); Edmonds and Kennedy (2013); Lapan, Quartaroli and Riemer (2012) and Eyisi (2016:92). These are quantitative, qualitative and mixed methods. The quantitative research approach is characterised by the

gathering of data with the aim of testing a hypothesis. The data generated are numerical, or, if not numerical, can be transformed into useable statistics (Byrne, Daykin & Coad 2016). The qualitative research approach is primarily exploratory research. It is used to gain an understanding of underlying reasons, opinions, and motivations. The mixed method approach involves the collection and analysis of both qualitative and quantitative data in order to test or further understand sections of the issue being studied (James & Slater 2014:61). The three research approaches may also be differentiated on their relationship with research paradigms. The interpretivism paradigm is predominantly connected with qualitative methods that place a great importance on credibility (Hesse-Biber 2010). On the other hand, positivism is associated with quantitative methods, whose research approaches largely belong to several possible alternatives concerning natural phenomena; which is a quantitative method. Pragmatism ontology supports mixed methods epistemology and converges diverse methods (both qualitative and quantitative methods) to develop understandings about the condition (Hesse-Biber 2010).

The present study adopted a qualitative approach in the form of a case study to obtain a comprehensive understanding of the security of ePHI in a public hospital in South Africa. It has been argued that the qualitative approach is suitable when the researcher intends to understand complex relationships and orientation to everyday events that are occurring in natural settings (Flick 2007:67). Based on the nature of research problem, research questions and research paradigm adopted in this study, a qualitative research approach was the most suitable approach for this study. According to Creswell (2013:122), the qualitative method is used when a problem needs to be explored or when there is a need for a complex and detailed understanding of an issue, and when there is a need to empower individuals to "share their stories and hear their voices". With the qualitative approach, the researcher was able to explore the security of ePHI and obtain insights from the participants based on their prior knowledge and experiences about the security of ePHI.

Hennink, Hutter and Bailey (2011:230) opine that qualitative approach enables the researchers to recognise issues from the point of view of the research participants, comprehend the issues from the perspective of the study participants, and understand meanings and explanations they attach to their behaviour, occurrences or objects. This is true because this approach enabled the researcher to obtain information from the participants about the security threats they encounter on a daily

basis. By using a qualitative approach, the researcher was able to fully describe the security control measures used in the hospital to secure and protect ePHI. This allowed the researcher to create a picture of what institutional leaders (hospital managers and stakeholders) need to know about the security threats to ePHI and how to best address securing them in future. Furthermore, this approach allowed for open questions and probing, thereby giving participants a chance to respond in their own words and allowing the researcher to engage more actively with study participants.

3.4 Research design

According to Lo-Biondo Wood and Haber (2017:150), a research design is defined as "an overall plan or blueprint for addressing a research question including conditions for maximising control over factors that could interfere with the study's desired result". The choice of a design depends on many factors, including research problem, purpose, aims, researcher's expertise and the researcher's desire to generalise the findings (Brink, Van der Walt & Rensenbury 2012:55; Hedges & Williams 2014:112). Creswell (2014b) defines research design as "the entire process of research, from conceptualizing a problem to writing research questions onto data collection, analysis, interpretation and report writing". Creswell (2014:11-15) discusses various research designs applied in quantitative, qualitative and mixed methods approaches. Figure 3.4 illustrates the research design inquiries.

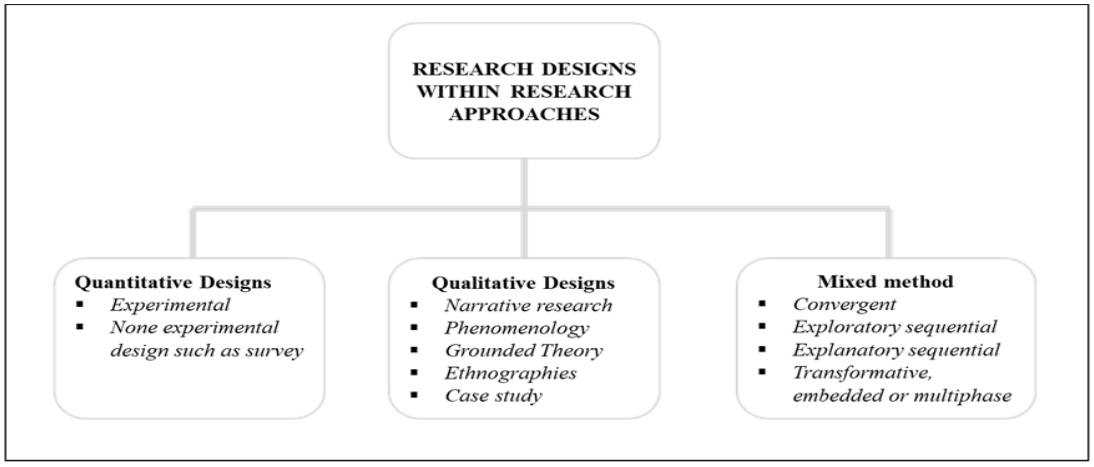


Figure 3.2 Research designs (Creswell 2014)

The choice of the research design to be employed in a study is based on a number of factors. These include the nature of the research problem, the worldview assumptions that the researcher brings into the study and the research questions that are addressed (Creswell 2007). Based on the research problem of this study, a case study design was adopted to obtain a comprehensive and in-depth knowledge about the security of ePHI in a public hospital. Denscombe (2010:54) refers to a case study as "a technique of thoroughly investigating a phenomenon for a while inside its ordinary location in a singular or multiple locations, using numerous approaches of data gathering, for instance interviews, observations or questionnaires". Case study research is a detailed exploration of a phenomenon in a real-world scenario (Yin 2013:332). There are two forms of a case study design known as single-case and multiple-case study. This study used a public hospital as the unit of analysis to collect data about the security of ePHI. In this way, the study adopted a single-case study because the objective of this study focused on the in-depth investigation into the security of ePHI within a public hospital. This design enabled the researcher to explore and discover the existing situation in the hospital in relation to the security of ePHI. Walker (2012:46) posits that case studies allow individuals to gather using different sources to capture information needed to understand the research problem that is being investigated. A case study design was aligned with the intent of this study, because the researcher employed different forms of data gathering methods to capture the information needed to understand security of ePHI in a public hospital in South Africa.

3.5 Population

Trochim, Donnelly and Arora (2016:155) and Bryman (2016:201) define a population as "the universe of units or a group that a researcher wants to generalise to, and from which a sample is selected". From the above definition, a population can be said to be the entire collection of people or things a researcher is interested in from which a sample is selected for analysis. The target population for the study included IT personnel, administrative workers and records management staff currently working in the hospital. The intent was to specifically focus on staff with relevant experience on the security of ePHI in order to obtain valuable and useful information. People in this population share at least one basic characteristic, which is the fact that they deal specifically with ePHI about patients, hospital computers and systems of the hospital.

3.6 Sampling method

Polit and Beck (2016:250) define a sample as "a subset of population elements (humans), which are the most basic units about which data are collected". According to the authors, the process of selecting the sample is called sampling, which is a process of selecting a small number of participants from the population of a phenomenon being studied (Pickard 2013:59). The researcher used purposive sampling to select IT technicians, network controllers, administrative clerks, and records clerks working in the hospital. This is because the purposive sampling technique enables the researcher to restrict the research to particular individuals who can provide the needed information about the security of ePHI. The study results were obtained from a total of 10 female and 5 male participants. Data saturation was reached on the 13th interview as no new data, themes or coding emerged. Total redundancy was confirmed at the 15th interview. Table 4.1 presents the purposively selected study participants from the study population:

Table 1: Summary of study population

Hospital unit	Sampled participants	No of selected participants
IT unit	Network controllers	2
	IT technicians	3
Administrative unit	Administrative clerks	7
Records management unit	Records clerks	3

3.7 Data collection method(s)

The qualitative study requires the researcher to collect data in a naturally uncontrolled setting. This ensures that the data collection process is extensive and relies on multiple techniques (Pickard 2013:66). Various data collection techniques are used to collect data in qualitative research. These include observation, interview, focus group discussion and content analysis. This study has employed three data collection methods to explore participants' views concerning the security of ePHI in the hospital. These are (i) semi-structured interview, (ii) document analysis and (iii) system analysis. Semi-structured interviews were conducted to gain rich data without the intrusion

of the researcher. The semi-structured questions consisted of open-ended questions, which allowed the researcher to probe participants to elicit additional information and tacit knowledge, which provided insight into the security of ePHI. All interviews were conducted at the hospital at a convenient time for the participants.

To complement the information gathered from the interviews, the researcher analysed relevant hospital literature, standards and organisation-specific documents, such as health security legislation, policies and regulations to check the existence of security measures pertaining to the security of ePHI. Furthermore, the researcher assessed hospital systems to check technical measures. The researcher developed an interview guide (see Appendix B) to retrieve information needed to understand the security of ePHI. These techniques were used to collect data from IT personnel, administrative workers, records management staff currently working in the public hospital. Triangulation of data collection techniques was intended to yield rich and in-depth data that enabled the researcher to provide both analytic generalisation and conclusions.

3.8 Data analysis method(s)

Data analysis entails categorising, ordering, manipulating, summarising and describing the data in meaningful terms (Brink et al 2012:170). Qualitative data analysis is a rigorous and logical process through which data are given meaning (Grove, Burns & Gray 2013:493). For the purpose of this study, data were transcribed verbatim and analysed with ATLAS.ti, version 8 software. This software enabled the researcher to analyse data by coding for themes. The five-step procedure was followed (Srivastava & Thomson 2009:188), which includes the following steps: (a) the researcher is immersed in the data by transcribing and re-reading transcripts; (b) identify emergent themes from the data. New themes were identified by means of open coding. (c) The data were then indexed in correspondence to the themes within the framework; (d) Charts are used to arrange the data that was previously indexed in the third stage. The use of charts and maps allowed the data to be classified under headings that relate to the thematic framework. (e) The final stage, mapping and interpretation, involved the development of a schematic diagram from the analysis to guide the interpretation of the data. It was important that any conclusions drawn from the data echoed the underlying attitudes, beliefs and values of the participants.

3.9 Trustworthiness

Trustworthiness is defined as the degree to which research data provides an accurate reflection or measure of the topic or variable under consideration (Murchison 2010:121). It is the extent to which an instrument measures exactly what it intends to measure. Trustworthiness is made up of a different set of criterion: credibility, which is equivalent to internal validity or matching what is observed with theoretical ideas; transferability, which is parallel to external validity or degree to which findings can be generalised across social settings; and conformability, which is used as a synonym of construct validity to mean the researcher's objectivity and neutrality. The term 'dependability' is used synonymously with reliability in qualitative research and neutrality (Riege 2003:76).

Credibility refers to the correctness and truthfulness of the data and information supplied by the research participant (Burns & Grove 2011:589). The researcher achieved credibility of the data and information by recording and note-taking simultaneously. The researcher used triangulation to serve as evidence that the research findings are credible.

Transferability refers to the potential for extrapolation, that is, the extent to which findings can be transferred to or has applicability to other settings or groups (Polit & Beck 2016:560). Transferability was achieved through a dense description of the demographics of the participants. The findings of this study could be applicable to other hospitals because a rich description of the results with supporting direct quotation of participants were included in order for other researchers to be able to make judgements about transferability.

Confirmability refers to objectivity, meaning the potential for congruence between two or more independent people about the data accuracy, relevance or meaning (Polit & Beck 2016:559-560). Tape recordings were used and field notes were taken during the interviews to increase the confirmability of the research.

Dependability refers to the establishment of data over time and conditions will be assured by collecting, recording, transcribing and translating information as accurately as possible and by providing a literature control, where appropriate (Polit & Beck 2016:559). To demonstrate this criterion, some direct quotations from participants' interviews were taken into account, accompanied by background information, such as time of the day, facial expressions and other relevant non-verbal cues.

3.10 Ethical considerations

Ethics is defined as "a number of honest values proposed by a person or society, consequently generally assented, and which provides guidelines and goals for behaviour regarding the proper practice concerning human experimentation by establishments, promoters, social researchers, and scholars" (Strydom 2005:57). The University of South Africa provides guidelines and policy documents that show what ethical considerations the researcher should follow (University of South Africa 2013). These documents ensure that the researcher avoids plagiarism and harming participants and non-participants either physically or emotionally.

The researcher adhered to ethical standards as set out in the research ethics policy of the University of South Africa (UNISA 2013). Permission to conduct the study was sought from and granted by the Department of Information Science Research Ethics Committee. Ethical clearance was granted (see Appendix D). Permission to conduct the research in the public hospital and interviews with participants was obtained from the Tshwane Research Committee. An informed consent form was provided to the participants to ensure that they were aware of the fact that their involvement was voluntary and that they could withdraw from the research process at any stage without any sanctions.

Anonymity and confidentiality of study participants were ensured during data collection and reporting the results as advised. Data collected were kept confidential and access to information related to the study was strictly controlled. Participants were also assured that the research results will be used only for the purposes of this study. Furthermore, study participants were assured that

personal identities such as names and surnames and the data gathered were going to be treated with extreme care and application for no other intention than scholarly.

3.11 Evaluation of the research methodology

Madsen (2013:193) states that limitations are the potential weakness that might limit the scope of the research findings. While undertaking this study, the researcher encountered several challenges which were methodological in nature. One of the challenges the researcher experienced, was access to the hospital. At first, the researcher targeted private hospitals to collect data for this study. A couple of private hospitals in Pretoria and Johannesburg were approached. However, some of the hospitals declined the application due to the sensitive nature of the research and deemed confidentiality of the specific data required (see Appendices H & I), and other hospitals did not respond to the application. The researcher resolved this challenge by approaching one of the public hospitals in Gauteng and permission to conduct research within the public hospital was granted.

Another challenge experienced during course of data collection, was access to hospital documents. The researcher struggled to gain access to various documents such as policies and procedures, official manuals, hospital plans and reports compiled by the public hospital. However, one of the patient records managers in the public hospital granted the researcher access to policy documents. In addition to these challenges, during the course of the interviews, some participants refused to be audio-recorded. However, the researcher resolved this challenge by writing down what the participants said. These challenges had an impact on the data duration. However, through the researcher's persistence, data were collected in a period of two weeks.

3.12 Summary

This chapter discussed the research methodology used in the study of security of electronic personal health information in a public hospital in South Africa. Specifically, the chapter deliberated on the research paradigms applied in social sciences and settled for the interpretivism paradigm, which is in consonant with the qualitative approach used for investigation. The researcher blended qualitative methodologies in conducting the study. The study population,

sampling procedures, data collection procedures, instruments for gathering data, data analysis methods, trustworthiness, in addition to ethical issues were presented and deliberated to provide an understanding of how the study was conducted. The next chapter discusses data analysis and presentation of the findings.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION OF FINDINGS

4.1 Introduction

The preceding chapter presented the research methodology for the study. In the previous chapter, the research methodology was reported, which included the philosophical position in which the study was conducted, the research approach and research design, data collection methods, data analysis methods, trustworthiness of the study and research ethics applied in this study. Having delineated the research methodology in the previous chapter, this chapter analyses data and presents the findings. Saunders, Lewis and Thornhill (2012:415) define data analysis as "the process of obtaining meaning from raw data and of discovering their implications". Creswell (2009) avers that data analysis is a key aspect of any research since it helps in drawing conclusions and generalisations from the data as it relates to the problem statement. Connoway and Powell (2010) concur with this view, and assert that the main purpose of analysing data is to summarise observations or data such that it provides answers to a hypothesis or research questions. The discussion and interpretation of the results are presented in Chapter Five. Data are analysed and presented as per the objectives of the study.

4.2 Data analysis

The data for this study were collected through structured interviews and analysed using ATLAS.ti 8 software and integrated thematically. All interviews were recorded using a voice-recording device. In addition, a field journal was also used to record the interviews in writing. The voice recordings and field notes were compared and transcribed. All of the participants' views and voices are presented in this study and all responses were quoted verbatim. These verbatim quotes form part of the evidence presented in this study. Furthermore, the researcher also visited the hospital to analyse hospital documents and systems. Data collected through document and system analysis were qualitatively analysed and presented in this chapter. Privacy, confidentiality and anonymity were ensured by assigning codes to the participants. Furthermore, the name of the hospital was not

mentioned. The codes were assigned according to the sequence in which the interviews were conducted as follows: Network Controller 1(NC-1), IT technician 1(IT-1), Admin Clerk 1 (AC-1), and Record Clerk 1 (RC-1).

4.3 Demographic profile of the participants

This section describes the demographics of the participants that made up the sample for this study. As highlighted in the previous chapter, 15 participants were selected using purposive sampling methods. Semi-structured interviews were conducted with the 15 participants and data were analysed and interpreted. The participants of the study were females and males who have been working at the hospital for more than one year as this was one of the criteria for sampling inclusion. Table 4.1 illustrates the demographic information of the participants:

Table 4.1: Demographic information of the participants

Quote no.	Job position	Years of experience	Highest level of qualification	Gender
NC-1	Network controller	7 years	Information Technology Certificate	Male
NC-2	Network controller	1 year, 9 months	National Diploma in Information Technology	Male
IT-3	IT technician	3 years	Microsoft Professional Certificate	Female
IT-4	IT technician	2 years	Technical support certificate	Male
IT-5	IT technician	1 year	National Diploma in Information Technology	Male
AC-1	Administrative clerk	4 years	Diploma in Admin & Business Management	Female
AC-2	Administrative clerk	10 years	Matric certificate	Female

AC-3	Administrative clerk	8 years	Certificate in Marketing	Female
AC-4	Administrative clerk	3 years	Matric certificate	Female
AC-5	Administrative clerk	5 years	Diploma in Administration	Female
AC-6	Administrative clerk	4 years	Certificate in Public Administration	Female
AC-7	Administrative clerk	8 years	National Diploma in Financial Management	Female
RC-1	Record clerk	9 years	National Diploma in Administration	Female
RC-2	Records clerk	10 years	Matric certificate	Male
RC-3	Records clerk	8 years	Matric certificate	Female

4.4 Presentation of the research findings

This section presents the findings and the themes that were extracted from the 15 interviews conducted within this qualitative study. This study made use of the deductive way of data analysis, which means that themes, categories and sub-categories were formulated prior to data analysis, based on the literature and personal view or experiences. The different parts of the data have been analysed together, in accordance with the five themes. These themes are (a) policy and regulatory framework governing the security of ePHI in the public hospital; (b) security threats to ePHI experienced by staff personnel in the public hospital; (c) security control measures undertaken by the public hospital to protect ePHI; (d) privacy issues associate with ePHI in a public hospital; and (e) recommended strategies for enhancing the security of ePHI in a public hospital. Table 4.2 provides a summary of themes, categories and sub-categories which emerged during the course of the interviews and which, in turn, inform the presentation of the findings of the study.

Table 4.2: Themes, categories and sub-categories

THEMES	CATEGORIES	SUB-CATEGORIES
THEME 1: Policy and regulatory framework governing the security of ePHI in a public hospital	1.1 Legislation and regulations	• PAIA Act • POPI Act • PAJA Act • NARSSA • GDoH PAIM • NH Act • Constitution of RSA
	1.2 Security standards	• Lack of knowledge of security standards • ISO27799 standard • Minimum security standards (MSS)
	1.3 Policy and procedures	• Lack of security policy • Administration policy • IT policy • Records management policy • Human resource policy • Medicine policy
THEME 2: Security threats to ePHI in a public hospital	2.1 Cyber security threats	• Worm viruses • Trojan horses • Shortcut viruses
	2.2 Technological threats	• Power failure • System failure • Poor network connection • Obsolete computers & operating system • Outdated hospital system

THEME 3: Security control measures used by the public hospital to protect ePHI	3.1 Hospital system(s)	• PAAB system • Metro-file system • Rx system
	3.2 User access control	• Authentication mechanisms • Password & username
	3.2 Technical security controls	• Antivirus program • Windows firewall • Security Audit log system • Data encryption
THEME 4: Privacy issues associated with ePHI in a public hospital	4.1 Privacy issues experienced by hospital staff	• Unauthorised access • Patients' data loss
THEME 5: Recommended strategies for enhancing the security of ePHI in a public hospital	5.1 Hospital plans to improve the security of ePHI	• System upgradation/migration
	5.2 Security improvements	• Upgrading computers • Upgrading PAAB system • Updating Windows operating system • Implementation of back-up system • Updating firewall & antivirus software • Network improvement • Implementation of security policy

4.4.1 Policy and regulatory framework governing the security of ePHI in a public hospital

This theme emerged with the following categories, namely: legislation, international security standards, and policy and procedures of the hospital. Healthcare providers are required by law to comply with relevant legislation to which they are subject. As already indicated in the literature review in Chapter Two, compliance with policies, procedures, and legislation and security standards is the primary concern in the healthcare sector to ensure the security of ePHI and maintain the security requirements of patient privacy and confidentiality. According to Tuyikeze and Pottas (2005:67), hospitals and healthcare centres in South African healthcare should develop legislation, standards and policies that regulate the security of patients' data. The following section presents the key findings in detail.

4.4.1.1 Legislation and regulations

The security of ePHI in healthcare sector in South Africa is impacted by various pièces of legislation. Participants were asked to identify pieces of legislation that govern the security of ePHI in the public hospital. The pieces of legislation identified by the participants are the Protection of Personal Information (POPI) Act, Promotion of Access of Information Act (PAIA), National Health Act (B+NH Act) and Promotion of Administrative Justice Act (PAJA) as the key legislation pertaining to the security of ePHI in the selected hospital. One of the participants (NC-1) elaborated that:

> *"Our hospital has established a number of legislation such as PAIA Act, POPI Act, PAJA Act and the National Health Act to govern the protection of patient's electronic health information. These pieces of legislation are useful to provide us with broad guidelines on how we should take necessary measures protect electronic personal health information that is stored and captured in the hospital system.*

However, despite the pieces of legislation being identified, Participant (AC-2) remarked that:

> *I don't have any idea about the legislation that is applied by the hospital to protect electronic personal information stored in the hospital system.*

Through document analysis, this study discovered other key legislation adopted by the hospital, which includes: National Archives and Records Service of South Africa Act, No. 43 of 2003

(NARSSA Act), the Constitution of the Republic of South Africa, No. 108 of 1996, section 195, and the Gauteng Department of Health Promotion of Access to Information Manuals Act (GDoH PAIM). These pieces of legislation were identified through ICT policy and records management policy of the hospital. These policies were further analysed. According to Williams (2005:117), the adoption of legislation to protect the privacy and confidentiality of patient information promotes the notion of accountability. The Constitution of South Africa states that healthcare organisations in South Africa are required to adhere to the stipulations of the relevant sections of PAIA, the NH Act, PAJA and the POPI Act.

According to Buys (2017:954), "the main purpose of the POPI Act is to protect any personal information which is processed by public and private bodies (including government)". The POPI Act states that any personal information collected by healthcare organisations in South Africa must be protected from loss, damage, and unlawful access. PAIA is more concerned about the right of access to records held by either public or private bodies for legitimate purposes. The purpose of passing the PAIA was to promote and enforce open access to information in possession of government entities or institutions. In the literature review (Chapter Two), Marutha and Ngulube (2010:10) indicated that the main aim of PAIA is to ensure the protection of people's rights. For example, patients in the public/private hospital have the right of access to information to their medical or health records. The PAJA is a pioneering legislation that intends to give the right to administrative action that is lawful, reasonable and procedurally fair as well as the right to written reasons for administrative action.

South African healthcare organisations are required to comply with PAJA. In healthcare organisations, this legislation aims to protect patients from unlawful, unreasonable and procedurally unfair administrative decisions. The NH Act aims to provide a framework for the healthcare system in South Africa. The Act provides for a number of basic healthcare rights, including the right to emergency treatment, the right to access healthcare services and the right to participate in decisions regarding one's health (NH Act 2015). This act aims to protect, promote, respect and fulfil the rights of South Africans with regard to health services. As a result, South African healthcare organisations must ensure that they comply with the NH Act. Responding to the probing question "How do you apply these existing legislation in the public hospital>"

Participants indicated that they apply these laws in their daily routine jobs. During the interview, one of the participants (NC-1) explained:

> *We usually refer to hospital legislation when we do our daily routine work to ensure that we follow the authentication protocols to help protect electronic personal information stored in the hospital system and to ensure that only authorised users have access to the information". Furthermore, in the hospital we're guided by this legislation to take necessary measures to protect patients' health information.*

4.4.1.2 Security standards

This category relates to the security standards pertaining to the protection personal information about patients in the public hospital. According to the Health Professionals Council of South Africa (2007), healthcare organisations in South Africa are required to set out security standards that provide protection for privacy of ePHI. Participants were asked to share with the researcher their knowledge on the ISO adopted by the public hospital to protect ePHI. One participant (NC-1) during the interview identified the ISO27799 standard as stated in the following extract:

> *The hospital has adopted the ISO27799 standard to guide hospital workers about the necessary control measures that should be undertaken to best protect the confidentiality and integrity of electronic personal health information captured and stored in the hospital system. This standard also help our hospital to meet regulatory requirements for patients' data Protection*

Other participants had no knowledge about existing ISO standards adopted in the public hospital to protect ePHI. For example, one participant (IT-3) said:

> *I don't have any idea about the security standards adopted by the hospital to protect electronic personal information of patients but according to the field of IT there are security standards that you have to apply such as disaster management standards. Honestly speaking, I have never heard about any International Security Standards that covers the protection of patients' health information in our hospital*.

Through document analysis, the study discovered that the public hospital has adopted a number of security standards to protect personal information about patients, including ISO 27799 (Health

informatics — Information security management), ISO 27001 (Information security management systems), ISO 27002 (Code of practice for information security controls) and Minimum Security Standards (system and network control). According to Tuyikeze and Pottas (2005), it is important for South African healthcare facilities to establish a set of formal security standards that address their security concerns and provide assurance to their patients. Gomes and Lapão (2008:56) support the view of participant (NC-1) that ISO27799 defines the guidelines for healthcare facilities and other custodians of ePHI on how best to protect the confidentiality, integrity and availability of such sensitive information (Gomes & Lapão 2008:56). The main objective of ISO 27799 is to provide security controls to protect PHI.

This standard aim is to provide clear, concise and healthcare-specific guidance on the selection and implementation of security control measures for the protection and security of PHI, and it is adaptable to the wide range of sizes, locations, and service delivery models found in healthcare (Fernández-Alemán, Señor, Lozoya & Toval 2013:543). Cavalli, Mattasoglio, Pinciroli, and Spaggiari (2004:297) state that because of the peculiarities of healthcare institutions and data, much analysis and design work needs to be done when implementing the generic ISO 27002 standard in the healthcare context. It follows that the same applies to the ISO 27001 standard. It is important that generic standards such as the ISO 27001 and ISO 27002 are supplemented to create industry-specific renditions, such as the ISO 27799 standard. Furthermore, the MSS are aimed at security standards to protect sensitive information of individuals.

4.4.1.3 Policy and procedures

Healthcare organisations are expected to establish internal policies and procedures which could adequately protect the confidentiality of patient information. Participants were asked about specific policies and procedures designed by the public hospital for the protection of ePHI. During the interviews, participants reported that the hospital has administrative policies, records management policies and medicine policies. However, they emphasised that the hospital does not have existing security policy that address the protection of ePHI. For example, one of the participants (IT-5) said:

Our hospital has implemented a number of policies and procedures that relates to administration, IT, records management, human resource management and medicine. Unfortunately, we don't have a clear formal security policy in the hospital that provides guidelines for establishing mechanisms to protect electronic personal information stored in the hospital system, but we usually attend the policy workshops whereby they guide us about compliance to hospital policies and procedures.

From the literature review in Chapter Two, Cucoranu et al (2013:89) mention that "the absence of appropriate policies and procedures for securing electronic health information can cause a number of conflicts such as authorised access unauthorised access, destruction, use, modification, or disclosure of sensitive health information". It is good practice for healthcare organisations to adopt security policies that set out principles and procedures that will ensure compliance with South African government legislation. Lu and Sinnott (2017:110) express their view that healthcare organisations need to develop and implement strict policies and procedures that provide detailed guidelines on how individuals may access and share personal information the hospital maintains.

4.4.2 Security threats to ePHI in a public hospital

This theme provides background information regarding the security threats experienced by the participants in the public hospital. The research findings related to the perceived security threats encountered by the hospital are further elaborated on in subsections 4.4.2.1 and 4.4.2.2.

4.4.2.1 Cyber-security threats

EPHI that is stored in the database of the healthcare organisations is vulnerable to a variety of cyber threats such as malware and malicious code attacks including viruses, worms, Trojan horses, logic bombs and trapdoors (Avancha et al 2012:67). In the literature review, Chapter Two, Eling and Schnell (2016:101) state that cyber threats arise from the use of IT and can damage the integrity, availability, or confidentiality of patients. Participants were asked to identify security threats they have experienced with regard to ePHI in the public hospital. Security threats identified

by participants during the interview include worm viruses, Trojan horses and shortcut viruses. For example, participant (NC-1) elaborated as follows:

> *The most common threats to our hospital computers and systems are Worm viruses, Trojan horse and we usually experience the short-cut viruses. These threats often cause hospital systems to malfunction, frequently crush, shutdown and send error messages and lower the speed of the hospital computers. And, most of the computers that are affected, are using the Windows XP operating system and remember Windows XP is no longer supported that is why it is a threat on its own.*

During the interviews, other participants emphasised that their computers are often attacked by computer viruses causing hospital systems to malfunction. For example, participant (IT-4) attested to this experience:

> *We usually experience minor security threats such as viruses from USBs and external drives that are used by staff members outside the hospital and these viruses often cause hospital systems to malfunction and most of the computers in hospital experiences frequent crashes, shutdown and error messages because of these viruses.*

In the literature review in Chapter Two, a series of studies indicated that threats such as Trojan horses, ransomware, worm viruses, malware, computer viruses and phishing are common in healthcare organisations (KPMG 2017; Wanyonyi et al 2017). These cyber threats have the potential to corrupt health information systems and damage patients' information. Cyber threats in healthcare organisations can expose sensitive patient personal information and lead to substantial financial costs to regain control of hospital systems and patient data.

4.4.2.2 Technological threats

Technological threats identified by the participants during the interview include power and system failure, poor network connection and obsolete software and hardware. One of the interviewees (AC-2) in the administrative unit expressed concern particularly about immediate loss of data resulting from power and system failure. The following excerpts, made by participants during the interview:

In the hospital…we usually experience power and system failure especially during winter seasons, and sometimes we even lose patients data. Due to lack of power and data backup systems in the hospital, sometimes it is difficult for us as clerks to recover patient's data especially after power returns. The system that we're using is an old version of the PAAB system, so most of the time is very slow…I think this is also because we're using outdated computers that operate with Windows XP. And, poor network is another problem that we're facing in the hospital…because of poor network connectivity, sometimes patients wait longer because we're struggling to open the system to capture and retrieve information about patients.

Another participant (RC-1) echoed a similar sentiment that:

The most common threats that we usually experience in the hospital…is power failure especially during winter and the hospital system that we're using is very slow most of the time System failure is also a major problem in our hospital. Most of the time our hospital computers are malfunctioning and shutting down unexpectedly. In addition this, network failure is also a major problem in the hospital especially after 20h00 in the evening.

According to Narayana et al (2010:203) in the literature review in Chapter Two, power and system failure, network failure and operating system failure present high-risk threats to hospital systems. Through system analysis, the researcher discovered that all computers in the administrative unit are obsolete and they use Windows XP operating system. The use of obsolete computers and operating systems have the potential to lower the computing speed. Responding to a follow-up question "How do you prevent and respond to security threats you have experienced?", all the record clerks and administrative clerks responded that they report threats to the ICT department and their hospital supervisors. One participant (RC-1) elaborated as follows:

Most of time…when we experience threats such as poor network, viruses, power and system failure…we usually contact and report these threats to the ICT department to deal with and solve them and sometimes we report these security threats to our hospital supervisors.

In contrast, participants from the IT unit indicated that security threats encountered in the public hospital are reported to a security company contracted by the hospital. For example, one interview participant (IT-4) highlighted that:

Security threats that we usually experience in the hospital…we report them to a security company that was appointed by the hospital for monitoring threats threatening the hospital systems and this company is also alerted automatically if threats attempt to attack hospital systems and they attend to these threats.

Coventry and Bradley (2018) advocate the view that IT personnel should prevent, mitigate and respond to security threats targeting the hospital systems, servers and networks.

4.4.3 Security control measures undertaken by the public hospital to protect ePHI

This section presents the security control measures used by healthcare organisations which were placed into the following categories: hospital system(s), access control and technical security controls. The following section presents key findings in detail.

4.4.3.1 Hospital system(s)

South African healthcare organisations have implemented different HIS to store, process and transmit electronic health information about patients. The study participants were asked to identify the system that is used by the public hospital to capture ePHI. Through interviews, the study discovered that the public hospital uses different systems. Systems identified during the interview are the PAAB, RX and Metro-file system. For example, a participant (AC-4) from the administrative unit emphasised this and said:

"In our hospital, we use three systems…which is the PAAB system, Metro-file system and Rx system. We use the PAAB system for capturing patients profile information, billing, registering new patients, admitting-discharging patients and scheduling appointments and we use the Metro-file system for retrieving electronic patient files, to request and book out the files and the Rx system for issuing medications prescribed by doctors and nurses in our hospital.

Through system analysis, the study established that the PAAB system is installed in all computers in the administrative unit, and the Metro-file system is installed in all computers in the records management unit, whereas computers from the hospital pharmacy are installed with the Rx system.

All these systems in the hospital contain personal information of patients. Côrtes and Côrtes (2011:139) state that every hospital uses different systems to perform daily routine activities such as capturing health information, processing payments, issuing of medication, admitting and discharging patients. The role of these HIS is to support clinical care, such as radiology and pathology, as well as monitoring, evaluation and administration purposes (Wright, O'Mahony & Cilliers 2017:52). Responding to the follow-up question, participants were asked to elaborate whether the PAAB system is integrated with systems of other public hospitals. Participants from the administrative unit emphasised that the PAAB is not integrated with other systems outside the hospital. One participant (AC-6) commented during the interview:

> *The PAAB system that we're using in the hospital is not integrated with systems of other hospitals, because different hospitals in Gauteng province use different systems, for instance Dr George Mukhari hospital use the Medicom system and other hospitals like Sefako Makgatho and Hellen Joseph use Clinicom and Medi-tech systems.*

Another participant from the IT unit mentioned that systems that are used in the public hospital are not integrated into one other. This was elaborated on by participant (IT-3):

> *Well…at the moment these systems that we're using are not integrated to each other, because each of this system performs different functions in the hospital.*

Kahn (2011:102) indicates that different HIS used by hospitals in South Africa are not integrated with one another due to low bandwidth. In the same vein, the Department of Health (South Africa) (2012b) reports that South African hospitals have adopted different HIS which are not readily able to be integrated with each.

4.4.3.2 User access control

Access control in the healthcare setting is crucial to ensure that only authorised users have access to ePHI stored in the hospital system. The overall goal of access control in healthcare organisation is to protect patient data (ISO 2008). Participants were asked to share their views on official staff with authority to access ePHI stored in the PAAB system. Participants indicated that administrative support staff and records and ward clerks have a legal right to access the ePHI stored

in the hospital system. One of the participants (RC-3) from the records management unit elaborated by saying:

> *In the hospital, all administrators including the revenue staff, records clerks and ward clerks have the authority to access electronic personal information of patients that is stored in the PAAB and Metro-file system, however IT, HR, finance and medical staff have limited access to the system containing patients' information.*

According to NHS (2007), it is essential for the hospital to grant only authorised personnel access to patients' information captured in the systems. In the same vein, Hau (2003:112) mentions that healthcare organisations therefore must allocate access rights appropriately – only to officials with authority to operate in respective tasks. As a result, unauthorised access to personal health information in the HIS may lead to various forms of discrimination and violation of fundamental rights. The participants were asked the follow-up question, "How is access to ePHI controlled?" All the study participants indicated that access to ePHI is controlled through authentication mechanisms. One of the participant (AC-7) from the hospital said:

> *In our hospital, we use various authentication and authorisation mechanisms to restrict and limit access to electronic personal information of patients and such mechanisms help to prevent unauthorised access and other breaches in the hospital.*

Authentication mechanisms are important to ensure that patients' data in the hospital system are protected from any unauthorised access that could interfere with the integrity of the hospital system. Based on this, participants were asked to indicate authentication mechanisms used by the public hospital to prevent unauthorised access to ePHI stored in the hospital system. Participants in the interview reiterated that username and password are authentication mechanisms used in the hospital to prevent unauthorised access to ePHI stored in PAAB, Metro-file and Rx system. It emerged from the interviews, as explained by one participant (NC-1) that:

> *In the hospital, we use password and username to control and limit access to and prevent unauthorised users from accessing our patient' health information stored in the PAAB and Metro-file system. Each user in the hospital has a unique username to log on the hospital system, while passwords are generated according to their desire. Our user passwords change*

regularly and users are required to generate password that contains at least eight characters, including lower and upper case, numeric and other special characters.

Collier (2014:240) emphasises that the basic standard requirements for user passwords include requiring that they are changed at set intervals, setting a minimum number of characters, and prohibiting the reuse of passwords. Through system analysis, the researcher also discovered that all computers in the hospital require a valid username and password before access to PAAB, Metro-file and Rx system is granted. Alban, Feldmar, Gabbay and Lefor (2005:108) state that username or identity (ID) with an associated valid password have been the most common user authentication mechanisms used in hospitals to protect personal information stored in the hospital system. The use of usernames and passwords within the hospital can ultimately prevent security breaches and threats by simply incorporating personal privacy regarding passwords and requiring users to frequently change personal passwords (Lemke 2013:25). According to Chen, Lu and Jan (2012:3378), the use of a valid password and username is a useful technique for healthcare providers establishing role-based access controls. Role-based access controls restrict and limit information to hospital users based on username and password assigned by the hospital system administrator. Through document analysis, the researcher also discovered that the hospital does not have a password policy that covers the strength of password and username.

4.4.3.3 Technical security controls

According to Jannetti (2014:8) and Pisto (2013:80), technical security controls refers to protecting the data and information system that resides within the health organisations' network. According to Blake et al (2017:28), healthcare organisations should employ various data security systems and security control measures to protect patient data. Technical controls are useful to ensure the integrity of patient health data by preventing unauthorised changes to information, breaches in IT network security, and ensuring that all users in hospital and disclosures are correctly authenticated. Healthcare organisations should ensure the protection and security of ePHI and set up technical control measures to prevent security threats, unauthorised access or any other breaches. Participants were asked the question, "What security control measures are in place to protect ePHI in the public hospital?" Through interviews, this study established that the public hospital uses

Windows firewall to block unauthorised access, and an antivirus program to prevent viruses and malicious codes attacking ePHI as well as the security audit log to trace who accessed the hospital system. For example, one participant (IT-5) concurred and said:

> *Uhm…one of the security measures that we use in the hospital is Windows firewall. The firewall is always active to block unauthorised users from accessing hospital computers and to prevent cyber-attacks threatening the hospital server, however it is not updated regularly and the antivirus program is installed in all computers to detect and prevents viruses…the name of the antivirus is Microsoft end point but because of network problems we usually take a while to update the antivirus. Another security measure that is used in the hospital…is the security audit log system. With this system, we're able to trace who accessed the PAAB and Metro-file system and what activities performed during a given period of time and what modification made to the records. The system gives log report so we are able to see everything.*

Furthermore, participant (AC-5) indicated that they use the data encryption technique to protect data and prevent unauthorised users from accessing ePHI. She said:

> *In the hospital, the antivirus program is installed in all the computers to prevent viruses and any other risks from attacking sensitive information captured in the PAAB system. Data encryption is also used in the hospital to prevent unauthorised users to access and modify or delete personal health information of patients. All electronic files containing personal health information of patients such as name, surnames, ID and medical history are properly encrypted and protected according the hospital standards.*

Through system analysis, this study established that the windows firewall on all the computers was activated but not up to date and the antivirus program was installed on all computers; however it was also not up to date. Technical security measures for access control ensure that only authorised users have legal access to ePHI and often require using unique user IDs, emergency access procedures, automatic log off, encryption, and audit reports or tracking logs of all activity on hardware and software (HIPAA 2015). According to Collier (2014:251), Ives (2014:52) and Bey and Magalhaes (2013:96), technical controls such as firewalls, antivirus, RFID, password and username credentials, cryptography, encryption and Intrusion Detection Systems (IDS) are useful techniques to prevent or limits access to patients' data as well as to maintain authentication,

integrity, availability, confidentiality, identification and privacy of patients' data. Study participants perceived existing security control measures in their hospital to be operating effectively and reliably to mitigate threats. The following verbatim extract from one of the interviews with participant (AC-7) confirmed that:

> *Security control measures that are used in the hospital are operating effectively, this is because our passwords contain special characters and no one from outside the hospital can copy and use our passwords and the antivirus program that is installed in our computers, it is effective and reliable…because we don't usually experience viruses affecting our systems and the firewall is also effective to block unauthorised users…so yah I can say they are reliable and effective.*

It is evident from the extract that the appropriate set of security controls used in the hospital is determined to be effective and reliable. Abouelmehdi, Beni-Hessane and Khaloufi (2018:5) advocate the view that healthcare organisations must develop and maintain the most effective, reliable and safe control measures and approaches to protect their patients' data.

4.4.4 Privacy issues associated with ePHI in the public hospital

As indicated above in the literature review (**C**hapter Two) Privacy, issues related to using ePHI in healthcare organisations include unauthorised access, data storage, data ownership, data sharing, user profile and misuse of health data. Privacy issues are at the focal point as emerging threats and vulnerabilities continue to be a problematic issue in healthcare organisations. With regard to privacy issues, participants complained about loss of patients' health data resulting from unexpected power outages and inadequate information backup. It emerged in the interviews, as explained by one participant (AC-6) that:

> *We usually experience loss of patients' health data during unexpected power outages such as load shedding, hardware failure and weather. Although, the hospital has installed the uninterrupted power supply (UPS) for power backup, but it is not sufficient and reliable to protect the hospital systems from damaging power problems and improve availability of patients' health data by allowing us to continue working without interruption of power outage.*

The inconvenience of health data loss can have negative implications for hospitals such as disruption of day-to-day functions of the hospital. Cucoranu et al (2013:13) affirm that unplanned power outages or sudden loss of power can cause serious issues such as loss of patients' data or damage to hospital systems. In contrast, other participants cited the issue of unauthorised access due to sharing of password-username and computers in the public hospital. One participant (NC-1) explained that:

> *"In the hospital, one of the privacy issues that was experienced was unauthorised access to our hospital system, due to the fact that access to the system was not restricted, and I remember at some point users were sharing one computer, for instance one computer was shared maybe by five users and they were forced to use one password and username…so this were one of the challenges causing unauthorised access to our systems…but currently we're working on improving the security of our systems to avoid any unauthorised access or modification and each user in the hospital is assigned with unique username and password"*

According to the Verizon Data Breach (2018), healthcare organisations are faced with the biggest threat from malicious insiders and unauthorised access to patient sensitive data (PHI and PHII information). Hassidim et al (2017:177) mention that one of the most common breaches to ePHI is the use of another person's credentials (username, pin and password) to access patient health information. This kind of act is regarded as both unethical and dangerous.

4.4.5 Recommended strategies for enhancing the security of ePHI in the public hospital

This theme emerged with the following categories: hospital plans to improve the security of ePHI and hospital security upgrades. The following section analyses the key findings in detail.

4.4.5.1 Hospital plans to improve the security of ePHI

The study participants were asked to share their knowledge with the researcher about the plans of the public hospital to improve the security of ePHI. One participant (IT-4) raised the point that the public hospital is planning to migrate from the PAAB system to the Medicom system to enhance the security of ePHI. She stated the following:

I have heard that the hospital is planning to upgrade PAAB system that is used for capturing and storing electronic patient information. According to the rumours the hospital is planning to migrate to another system which is the Medicom system. However, it has not been officialised when this system will be implemented in our hospital,

On the same note, participant (NC-2) said:

"The hospital is planning to introduce a new advanced system that provides better security… a system that will prevent patients waiting and long queues in the hospital"

The most important consideration for healthcare system migration is the security of ePHI. However, through document analysis, this study established that no reports or memorandums compiled by the hospital outlined the implementation or migration of a new system.

4.4.5.2 Security improvements

Study participants were asked to indicate strategies that the public hospital could adopt to improve the security of ePHI. Participants of this study suggested the need for the public hospital to upgrade computers and update the antivirus program and Windows firewall regularly to combat new viruses and protect hospital computers against hackers. Within the parameters of this study, participants suggested that the public hospital should develop a formal security policy to improve the security of patients' data. The following extracts from interviews provide further illustration on suggestions made by study participants. For example, one participant (IT-5) clearly suggested that:

The hospital should upgrade all hospital computers and the antivirus program and windows firewall should be updated regularly and enable the updates to run automatically or manually to prevent new viruses attempting to attack the hospital systems and block unauthorised users. The hospital should improve the performance of network and the hospital managers and supervisors should develop a formal policy about the security of patient's data, which guide us on how patient data should be handled, protected and accessed in the hospital.

On the same note, it was suggested by participants of this study that the public hospital should implement a biometric system and a back-up system, and upgrade the hospital system. Participants also suggested the need for the public hospital to improve network connection. For example, one participant (AC-1) further recommended that:

> *The hospital should the install the biometric system to strengthen the security and upgrade the PAAB system or migrate to other systems such as Medicom or Meditech because the PAAB system that we're using is old, outdated and is very slow and lastly the hospital should implement a proper back-up system that we can use to recover patients' health information in case of power outages and load shedding and also to improve the network connectivity because our network is always poor and slow.*

In the literature review (Chapter Two), Conaty-Buck (2017:64) suggests that healthcare organisations should consider improving cybersecurity through training staff, using software updates promptly, implementing cyber security technologies, controlling system access, using passwords, regular risk assessment and data recovery. HIPAA (2015) suggests that healthcare organisations should put precautionary measures in place when hosting sensitive patient data, including limited facility access with access controls in place and security policies governing use and access to hospital systems, electronic media, and any attempts at sharing, removing, disposing, and re-using electronic media or ePHI. In addition, cohesive security and staff guidelines and comprehensive training are necessary to improve the security of ePHI.

4.5 Summary

This chapter dealt with data analysis and presentation of the findings. The presentation of findings was based on themes derived from the research questions and subsequent research objectives reflecting the policy and regulatory framework governing the security of ePHI in the hospital, security threats to ePHI, security control measures used by the hospital to protect ePHI, privacy issues experienced associate with ePHI and suggestions to enhance the security of ePHI in the hospital. The analysis involved the presentation of sampled IT technicians, administrative clerks and records clerks. This study highlighted the demographic information of the participants and the fundamental findings revealed that key legislation such as the POPI Act, PAIA, PAJA, the NH

Act, the NARSSA Act, ECT Act and the Constitution of the Republic of South Africa Act have been adopted in the public hospital for the security of ePHI.

The International Security Standards such as ISO 27799, ISO 27001 and ISO 27002 are used in the public hospital for the protection of ePHI. Policies found in the hospital had more to do with administration, IT, records management, HR and medicine. Some of the participants involved in this study acknowledged that the public hospital does not have a clearly defined security policy that addresses the security and protection of ePHI. It is clear from the findings of this research study that the public hospital uses three systems known as the PAAB, Metro-file and Rx systems and these systems are not integrated with each other as they perform different functions. Authentication mechanisms such as passwords and usernames are utilised by the public hospital to control access to ePHI. It was thus found that the public hospital is faced with a multitude of threats such as cyber and technical threats. The study discovered existing countermeasures used in the public hospital to protect ePHI against various threats and risks. The next chapter discusses and interprets the findings in line with the research objectives and the literature reviewed.

CHAPTER FIVE

DISCUSSION AND INTEPRETATION OF FINDINGS

5.1 Introduction

The previous chapter dealt with the analysis and presentation of data. This chapter discusses and interprets the findings resulting from this study on the security of ePHI in a public hospital in South Africa. Ofulla (2013) describes discussion of findings as "a means through which the concepts that were examined and were observed by a researcher in the course of the study can be better understood; it also provides a theoretical conception that can serve as a guide for further researchers". Study findings are considered in view of the research problem and objectives presented in Chapter One as well as the literature review. The findings of this study are based on the analysis of data obtained through the process of semi-structured interviews of 15 participants who are currently employed by the public hospital. The process of data discussion and interpretation is important in presenting the key issue that were under the spotlight in the research project. Data interpretation in this chapter followed the order in which the results were presented and analysed in chapter four. The summary of major findings, conclusions and recommendations are covered in the last chapter, Chapter Six.

5.2 Discussion and interpretation of findings

This section covers the discussion and interpretation of findings. The discussion of the findings was guided by the research objectives of this study. The discussion themes were drawn from the following research objectives:

- Analyse existing policy and regulatory framework governing the security of ePHI in a public hospital in South Africa
- Assess the security threats to ePHI in a public hospital in South Africa
- Examine security control measures undertaken by the public hospital to protect ePHI
- Assess privacy issues associated with ePHI in a public hospital in South Africa
- Recommend strategies for enhancing the security of ePHI in a public hospital in South Africa

5.2.1 Demographic profile of participants

This section provides a brief overview of the demographic information of the participants. Demographic information is useful to help the researcher understand the characteristics of the participants. Demographic information involves personal characteristics of participants such as gender, age, occupation, years of working experience and the level of education. They assist the researcher in developing strategies for the target population (Brink et al 2012). Table 4.2 illustrated the demographic information obtained from study participants. The study comprised 15 participants currently employed by the public hospital. Participants were asked to provide demographic information on their gender, level of education, years of service and position held in their hospital. The results from interviews on gender indicated that there were proportionally more female participants than male participants. As a result, there was an imbalance between males and females who participated in this study.

Findings of the current study on the level of education showed that participants in this study hold IT qualifications, whereas other participants hold administration qualifications and matric certificates. This result demonstrates that the public hospital has realistically qualified staff. Findings of this study on years of services revealed that participants in the public had spent between 1 and 10 years in their current job. This study also found that other participants had spent 5 to 10 years working at their respective stations, which meant that they are more knowledgeable about the security issues the hospital experiences with regard to ePHI stored in the hospital system and some of the participants had spent 1 to 4 years working in the hospital. The results presented above on the position held by participants in the public hospital revealed that participants held the position of network controller, IT technician, and administrative clerk and records clerk. The participants involved in the study were from different divisions such as ICT, administration and records management.

5.2.2 Policy and regulatory framework governing the security of ePHI in a public hospital

This section discusses the key legislation, security standards, and policies pertaining to the security of ePHI in a public hospital.

5.2.2.1 Legislation and regulations

The literature review (Chapter Two) indicated that legislative and regulatory frameworks are an essential tool for improving health governance at the country level. Without legislation and regulations, authority is not set and the privacy, confidentially and other threats and risks affecting patient health information in electronic platform are compromised. The findings of the study revealed that the studied hospital operates within various legislation and guidelines in protecting ePHI. The studied hospital is a public hospital which operates and is governed under the stipulated national legislation. The researcher verified this by asking the one of the participants (NC- 1) who confirmed that the ePHI is protected within the stipulated legislation.

The key findings in this research highlighted that the POPI Act, PAIA, the NH Act and PAJA are adopted in the public hospital for the protection of any sensitive information about patients. Furthermore, the study participants indicated they apply existing legislation in their daily routine work to ensure the protection of sensitive information. From the document analysis in section 4.4.1.1, the hospital documents indicated that key legislation (NARSSA Act, Constitution of RSA and GDoH PAIM Act) were adopted in the public hospital.

As was highlighted in the literature review in Chapter Two that South Africa has specified and comprehensive legislation and regulations that govern the security of patient data in healthcare organisations and facilities. De Bruyn (2014) indicates that national key legislation such as the POPI Act, PAIA, PAJA and the NH Act are among the major national policy documents that shape the way electronic healthcare information is being accessed and used in hospitals and other healthcare facilities. These laws and regulations prohibit the disclosure of sensitive information about private individuals in the healthcare sector. As a result, South African hospitals and clinics are required to adopt these national laws and legislation. The findings of the current study also indicated that participants apply these pieces of legislation in their daily routine work and they are guided by these pieces of legislation with regard to the protection of ePHI.

5.2.2.2 Security standards

The literature indicated that healthcare organisations should adopt relevant security standards and frameworks to protect PHI stored and accessed electronically in HIS. The security standards provide guidance to healthcare organisations and other custodians of PHI on how best to protect the confidentiality, integrity and availability of their information (Tyali & Pottas 2011). The standards cover the fundamental requirements of information management systems, and provide guidelines and principles for the implementation of such systems. The findings revealed that other participants had no knowledge about existing security standards adopted in the public hospital to protect ePHI. However, it was found that ISO 27799 is used to benchmark the protection of ePHI in the public hospital. Findings from document reviews in section 4.4.1.2 revealed that ISO 27001 and ISO 27002 and the MSS were also adopted in the public hospital to protect ePHI. These security standards are more concerned about the security and protection of patients' health information that is stored and captured in healthcare systems.

In the literature review in Chapter Two, Coleman (2010) stressed that healthcare organisations should implement and develop these security standards to ensure that a minimum requisite level of security is appropriate to organisation's circumstances. These standards protect the confidentiality, integrity and availability of personal health data of patients. As indicated in the literature review (Chapter Two), the adoption of security standards by healthcare organisations can contribute to the safe adoption of new health technologies in the delivery of healthcare services. As a result of implementing these security standards, healthcare organisations across the globe can expect to see the number and severity of their security threats and risks being reduced, allowing resources to be redeployed to productive activities.

5.2.2.3 Policy and procedures

Healthcare organisations need to ensure that an appropriate and effective security policy is developed and put into practice throughout the organisation to safeguard patients' health data. HIPAA (2015) affirms that healthcare organisations should formulate formal security policies which should be reviewed regularly to keep pace with new technological advances and

legislative requirements. The security policy should address the password and username management, ePHI storage and access, use of encryption and privacy filters. Knapp and Ferrante (2012:67) assert that security policies are a critical safeguard to help employees understand how they need to behave with respect to protecting personal information and systems.

It was established in this study that the public hospital has clearly articulated written policies and procedures related to administration, IT, records management, human resource management and medicine. However, it was disclosed from the interviews that the public hospital did not have a formal security policy addressing the protection and security of ePHI in the public hospital. This is similar to the findings of Mehraeen, Ayatollahi and Ahmadi (2016:49) which indicate that university hospitals in Iran do not have a security policy addressing the security and access to patients' information. According to the administrative procedures, hospitals and other healthcare facilities are recommended to be equipped with detailed security policy documents (Mehraeen et al 2016:49).

As mentioned previously in the literature review (Chapter Two), the absence of security policy can lead to harmful security results such as loss of confidentiality, integrity or availability of ePHI. The review of the literature affirmed that a lack of security policy and procedures in the hospital for securing electronic health information can cause a number of conflicts such as authorised access unauthorised access, destruction, use, modification, or disclosure of sensitive health information (Cucoran et al 2013:89). Asogwa (2012:198) notes that databases containing personal information, financial and medical records can pose security, confidentiality and privacy violation challenges if proper access and security precautions are not put in place in the form of a policy. Peikari, Ramayah, Shah and Lo (2018:102) point out that health organisations are required to institute security policies and procedures to train their employees on information security issues such as potential threats and penetration techniques, employees' responsibilities on protecting the security of the information, required skills to deal with security threats.

5.2.3 Security threats to ePHI in a public hospital

This section discusses the main findings that emerged from the data in relation to the security threats experienced by the participants in the public hospital.

5.2.3.1 Cyber threats

Cyber threats are a growing threat to the healthcare industry, causing a massive data loss and monetary theft but also attacks on healthcare systems. According to the literature reviewed in Chapter Two, Jalali and Kaiser (2018:10059) stress that cyber-security threats are a growing threat to the healthcare industry in general and hospitals in particular. Cyber threats to organisations such as healthcare organisations present a range of damages that include reputational damage, financial gain and fraud, commercial advantage and/or economic and political damage (Scully 2011:201). In the context of the conceptual framework discussed above, the researcher noted that ePHI is vulnerable to various cyber threats. The findings of the study in section 4.4.2.1, on the security threats, revealed that worm viruses, Trojan horses, and shortcut viruses were the most perceived cyber threats encountered in the public hospital. According to Cucoranu et al (2013:14), shortcut viruses are regarded "as computer programs that can replicate themselves and spread from one computer to another; they are written intentionally to alter a computer's operation and almost always corrupt or modify files on targeted computers", whereas Trojan horses are "malicious applications masquerading as legitimate software that can grant hackers unauthorised access to computers". Worm viruses are stand-alone malware applications that replicate to spread to other computers, usually through computer networks (Cucoranu et al 2013:14). According to the findings of this study, these threats cause hospital computers to shut down unexpectedly, crash as well as operate at a lower speed.

Empirically, Ayatollahi and Shagerdi (2017:41) conducted a study on information security risk assessment in hospitals. The findings of their study found that computer viruses and Trojan horses were ranked among the major threats challenging public hospitals in Iran. The result was coherent with the previous studies reported that Trojan horses, ransomware, viruses, computer worms and malware are the most common cyber threats in healthcare organisations (Ponemon Institute 2016; KPMG 2015; Cooper & Collman 2005).

5.2.3.2 Technological threats

In the literature review (Chapter Two), it was stated that Narayana et al (2010:203) argue that technological threats present high-risk threats to hospital systems. These threats may have serious implications for healthcare-related facilities in general and healthcare service providers in particular. Findings from the interviews regarding the security threats faced by study participants (see section 4.4.2.2) revealed some pronounced technological threats encountered in public hospital, including power and system failure, network connection failure, outdated computers and operating system and outdated hospital system. According to the findings, these threats cause hospital computers to malfunction and shutdown unexpected. The findings form a study by Samy, Ahmad and Ismail (2010:203) showed that the most significant security threats to health data were power failure, system failure and network failure.

Furthermore, Narayana et al (2010:203) discern that power outages and system failures are among the most critical threats to HIS in hospitals. These technological threats can greatly affect the performance of HIS. According to the World Health Organisation (2018), power and system failures can cause interruptions in the use of essential medical and diagnostic devices, for instance, and may limit communication, both within healthcare organisations and between patients and healthcare providers. The participants in the administrative unit further indicated that security threats encountered in the hospital are reported directly to the ICT department and their respective hospital supervisors, whereas participants from the ICT unit indicated that technical problems are reported directly to the security company which has been hired by the hospital.

5.2.4 Security control used by the public hospital to protect ePHI

This section discusses the key findings that relate to hospital system(s), access control and technical security controls. The following section discusses these findings in detail.

5.2.4.1 Hospital system(s)

Asij and Nallusamy (2014) define hospital system as "the application of information processing involving both computer hardware and software that deals with storage, management, transmission, retrieval and sharing of information related to the health of individuals or the activities of organisations that work within the health sector". In healthcare environment, a number of HIS have been developed to assist healthcare organisations to provide efficient and quality healthcare services (Fiza, Lizawati, Zuraini & Narayana 2016:2). The literature review in Chapter Two indicated that South African hospitals have implemented different HIS in the public healthcare sector to improve the quality of healthcare and support direct patient care (Cilliers & Wright 2017:36). Seahloli (2016:83) indicates that public and private hospitals in South Africa have partially implemented HIS for the purpose of capturing, storing and managing patient health data.

The qualitative interviews with participants showed that PAAB, Metro-file and Rx were systems used in the public hospital to automate the patient administrative functions such as capturing patient profile information, retrieving patient files, billing, dispatching medication and scheduling appointments. However, the findings revealed that these systems are not integrated as they perform different functions and they are not integrated to other external hospital systems. According to Beaumont (2011:101), PAAB is a system that is owned by the Department of Health (DoH). The system is used mainly for administration; a clinical data-recording module has been added but it lacks the functionality to enable the data to be used in an integrated manner. However, the system does not currently support electronic linkage to pharmacy systems, direct importing of laboratory or radiology results, and decision support. Furthermore, the Rx system is a pharmacy dispensing and stock control system that was funded by the US Centres for Disease Control and Prevention (CDC), and implemented in clinics and hospitals in five provinces (World Health Organisation 2012).

5.2.4.2 User access control

Access control is an important security issue for healthcare organisation. Confidentiality is a main concern when it is related to patient clinical information that needs to be private. It is essential to protect this information from unauthorised access and, therefore, misuse or legal liability (Ferreira,

Cruz-Correia, Chadwick & Antunes 2007:62). Access control makes it possible for healthcare organisations to control, restrict, monitor, and protect the integrity, availability and confidentiality. A recent study by Gordon, Fairhall and Landman (2017:707) argued that access to PHI should be limited to persons who absolutely require it, in keeping with "need-to-know" policies. In the case of the public hospital under study, the findings revealed that administrative support staff, including admin staff record clerks and ward clerks working in the public hospital are permitted to access to ePHI stored in the PAAB and Metro-file system. However, according to the findings, IT staff, HR staff and financial staff have limited access to ePHI. A study by Mahmood (2010:50) shared similar findings that IT engineers, policy makers and medical staff have limited and restricted access to electronic health information in Blekinge healthcare.

The findings discovered that authentication and authorisation were the methods used in the public hospital to technically protect ePHI from unauthorised access and modification or disclosure. Rana, Kubbo and Jayabalan (2017:273) stress that healthcare organisations need to adopt authentication mechanisms that properly protect patients' data from unauthorised access. This research found out that access to ePHI in the public hospital is protected. According to the findings, a password and username were authentication methods used in public hospital to technically protect ePHI against unauthorised access and modifications. Chen, Lo and Yeh (2012) emphasise that the use of usernames and passwords can ultimately prevent security threats by simply incorporating personal privacy regarding passwords and requiring users to frequently change personal passwords. Cipresso, Gaggioli, Serino, Cipresso and Riva (2012) advocate that a good password contains at least six characters (mixed lower- and upper-case) as well as numbers, and possibly even punctuation marks.

This is similar to the findings by Mahmood (2010:50) whose findings revealed that access to patients' health information in Blekinge healthcare is controlled by usernames and passwords. The username is the actual name of the employee in the healthcare system while password is generated according to their desire. The password used by employees changes every month. Ball, Chadwick and Mundy (2003) caution that usernames with an associated password have been the most common user authentication mechanisms used in healthcare organisations. In healthcare organisations, it is important to control the information that is accessible to users, as it is important

to determine who has permission to access the information and what type of information is accessed to restrict access to information and ensure that users only access the information they need according to their functions, thus enabling authentication and authorisation of systems to be controlled (Rindfleisch 1997:9).

5.2.4.3 Technical security controls

Technical security controls refer to "protecting the data and information system that resides within the health organisations' network" (Liu, Musen & Hou 2015:1473; Jannetti 2014:6; Lemke 2013:26). These security controls are useful for healthcare organisations as many threats and breaches occur via electronic media such as computers, laptops or portable electronic devices (as previously mentioned in the literature review (Chapter Two)), defensive security measures within this category include but are not limited to items such access control systems, password, Audi trails, antivirus, encryption, decryption, firewalls, Intrusion Detection System (IDS), Frequently Identification (RFID), Secure Sockets Layer to evade security threats and risks (Cooper & Collman 2005:103). Failure of such security measures may disrupt business continuity and diminish operating efficiency. The literature review indicated that healthcare organisations are required to deploy technical security measures to avoid patients' data protection breakdowns that might result in enormous and costly damages.

It was clear from the findings of the current study that Windows firewall is used in the public hospital to block unauthorised users from accessing ePHI and Microsoft end-point antivirus program is also used to detect and prevent any malicious codes such as viruses, Trojan horses, and Worms attacking the hospital systems. However, the findings revealed that the Windows firewall and antivirus program deployed in the public hospital were not updated regularly. The antivirus program can detect, remove and protect hospital computers and networks against viruses, spyware and malware-based attacks; however, to be effective they need to be properly updated and maintained. They have to be correctly configured for automated, regular virus definition updates and file scanning (Cadick 2005). Furthermore, the Windows firewall should be updated regularly to block or prevent unauthorised users from accessing private hospital networks or limiting access to the outside from within the hospital network (Kwon & Johnson 2013:48).

Study findings from the interviews confirmed that electronic files containing PHI of patients are properly encrypted and protected according to standards imposed by the hospital, so that they are not disclosed while in transit from the patient to hospital server. Health IT (2012:89) asserts that healthcare organisations should also ensure that information captured in the hospital system is encrypted as this can help to prevent outside access to private networks, or limiting access to the outside from within the network. According to HIPAA (2015), encryption is one of the most useful data protecting mechanism for healthcare organisations. By encrypting patients' data in transit and at rest, healthcare providers and stakeholders make it more difficult (ideally impossible) for attackers and cyber criminals to decipher patient information even if they gain access to the patient data.

Furthermore, findings on security control measures (section 4.4.3.3.) showed that the security audit log system is deployed in the public hospital to trace who accessed the hospital system and what patients' health information accessed and any modifications the records made. The study findings corroborate those of Wu et al (2017) who studied EHR audit trails in clinics. They found that ambulatory clinics in the Western United States use HER security audit trails log to provide supportive evidence to the known workflow changes. In the healthcare setting, the security audit log is highly relevant evidence as to who accesses the hospital system, what health information is accessed, what entries were made and/or changed, by whom and when (Scott 2011:189). HIPAA (2015) stresses that security audit trail logs should be maintained in accordance with recordkeeping standards and all electronic applications that interface with ePHI should fall under the remit of the audit trail in order to mitigate the risk of security threats, data breaches and fraud. Furthermore, the findings of the current study showed that existing security control measures used in the public hospital are perceived to be operating effective and reliable to protect ePHI against threats.

5.2.5 Privacy issues associated with ePHI in a public hospital

According to Fernandez-Aleman et al (2013:02), information privacy issues have long been debated in the context of technological change and electronic databases in healthcare. The use of health technologies and the integration of HIS in healthcare organisations give rise to issues

relating to privacy of electronically transmitted and stored information about patients. Findings of this study in section 4.4.4 revealed losses of patients' health data resulting from unexpected power outages and inadequate power backup. According to a study performed by Cucoranu et al (2013:22), unexpected/unplanned outages can result in patient data loss, therefore it is crucial for healthcare providers to implement measures that could prevent future occurrences of such outages.

Furthermore, findings on privacy issues, as presented in section 4.4.4, revealed that unauthorised access to ePHI was encountered when computers, passwords and usernames were shared among staff employees in the public hospital. As mentioned above in the literature review (Chapter Two), unauthorised access to ePHI remains a chronic issue in healthcare sector. A recent study by Hassidim et al (2017:180) on examining the prevalence of password sharing among healthcare professionals in Jerusalem found that medical staff members reported having used another medical staff member's password and username to access EHR systems in the hospital.

Password and username sharing represents one of the greatest threats in healthcare sector (Hassidim et al 2017:181). The practice of sharing login credentials (username, pin or password) in healthcare among staff may endanger the hospital and potentially lead to risky consequences such as unauthorised access to sensitive information and decrease in data safety. As a result, proper protection of user credentials is vital in healthcare organisations. HHS (2017:112) points out that the actual implementation of a security policy that prohibits the sharing of passwords and usernames among staff members in the hospital must be enforced by sanctions on workers violating their predefined permissions and rules. Complying with the principle of limiting the exposure of ePHI to the minimum necessary, the above-mentioned regulations require a clear definition of each worker's role and access privileges. This means that there is a need to authenticate the identity of each staff member, control his or her access to patient data and audit, and trace any editing or modification of data, including accesses for retrieval only, of ePHI (HHS 2017:112).

5.2.6 Recommended strategies for enhancing the security of ePHI in a public hospital

This section discusses the key findings based on strategies recommended by participants to improve the security of ePHI in a public hospital. The findings on hospital plans to enhance the security of ePHI and recommended strategies for security improvements are discussed as follows:

5.2.6.1 Hospital plans to improve the security of ePHI

The findings of the study in section 4.4.5.1 on hospital future plans revealed that the public hospital is planning to migrate from the legacy system, which is the PAAB system, to a new system such as Medicom or Meditech. These systems that will enhance the security of ePHI in the hospital.

5.2.6.2 Strategies for security improvements

The present study discovered a broad range of strategies recommended by study participants for enhancement of the security of ePHI in a public hospital. The findings presented in Chapter Four, suggested that the public hospital should implement the back-up system and data recovery system that will assist to recover patients' health information in case of power outages and loadshedding. It was also proposed that the public hospital should regularly update the antivirus program and the Windows firewall and set the updates automatically or manually. According to HIPAA (2015), it is crucial for healthcare organisations to regularly update the antivirus software and firewalls, because the computers in hospitals and healthcare facilities are regularly threatened by new viruses and attacks.

The results in this study suggest that all the computers in the public hospital should be upgraded and installed with the latest Windows 10 operating system to improve the speed and performance of the computers. In addition, there is general consensus that the hospital should install the Biometric system to improve the security and access to ePHI. The results of this study revealed the need to further upgrade the PAAB system or migrate to another system such as Medicom or Meditech. Furthermore, it was also suggested from this study that hospital network connection should be improved. The strategies raised in the interviews related to the establishment of the security policy. It was revealed in the interviews that hospital managers and supervisors should

draft a security policy that addresses how ePHI should be handled, accessed and protected against various threats and risks.

5.3 Summary

This chapter described in detail the discussion and interpretation of the findings. Study findings were supported with literature. The main themes of the study were discussed and interpreted in line with the subsequent research objectives. The discussions and interpretations were based on the study's research problem and the theories underpinning the study. The findings of the present study concur to the documented evidence found in related literature review. The next chapter presents the summary of major findings and conclusions on the findings. It also gives recommendations based on the findings of the study which are directed at the public hospital with regard to the security of ePHI. The chapter give the suggestions for further research.

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

"It always seems impossible until it is done"

Nelson Mandela

6.1 Introduction

The preceding chapter presented a discussion and interpretation of the study findings. This chapter provides a summary of findings that emanated from the study and reaches conclusions in accordance with study objectives. Denscombe (2007:110) points out that the summary and concluding chapters aim to draw together different threads of a research in order to reach a general conclusion and suggest a way forward in addressing the research problem. The final section of this chapter provides specific recommendations in an effort to further improve the security of ePHI in a public hospital. The recommendations are based on the findings presented in Chapter Four and their interpretation and discussion presented in Chapter Five.

According to Lam (2012), conclusions and recommendations have to reflect research problem and research objectives addressed in the study and relate the findings to the reality and set directions for future research. Lastly, this study will offer suggestions for future research. According to Habib, Pathik and Maryam (2014:110), topics for future research can be identified based on the limitations, methodologies, statistical tools, challenges, and findings of the study. This study was conducted in a public hospital in South Africa, with the purpose of exploring the security of ePHI. The study adopted a qualitative research approach because the researcher needed to obtain information from participants through exploration of the challenges they experienced with regard to the security of ePHI in a public hospital. As already delineated, the objectives of the study were to:

- analyse existing policy and regulatory framework governing the security of ePHI in a public hospital in South Africa
- assess the security threats to ePHI in a public hospital in South Africa
- examine security control measures undertaken by the public hospital to protect ePHI
- assess privacy issues associated with ePHI in a public hospital in South Africa

- recommend strategies for enhancing the security of ePHI in a public hospital in South Africa

6.2 Summary of the findings

This section presents a summary of the findings for the six research questions addressed in this study. The study findings were gathered through semi-structured interviews with IT technicians, records clerks and administrative clerks and were analysed and presented in Chapter Four with the aim of reporting all research responses accurately as proof for the study. The study findings were then interpreted and discussed in Chapter Five through the logical use of core themes, categories and sub-categories that were developed from the study outcome. The summary of findings is presented in this section based on the objectives of the study that were introduced in Chapter One (see section 1.4). The presentation of these objectives is preceded by summary of demographic profile of participants.

6.2.1 Policy and regulatory framework governing the security of ePHI

The first research objective of this study intended to analyse policy and regulatory framework governing the security of ePHI in a public hospital in South Africa. It was necessary to understand if the public hospital has own legislation pertaining to the security of ePHI. Chapter two of this study discussed the key legislation, security standards and policies aimed at protecting patients' data in South African healthcare organisations. It was established from interviews that pieces of legislation such as the POPI Act, PAIA, PAJA and the NH Act were adopted in the public hospital. Reviewed documents revealed that the Constitution of the RSA, the GDoH PAIM Act and NARSSA Act were also adopted in the public hospital to govern the security of ePHI. The study found that participants were guided by the said existing legislation with regard to the security of ePHI. Looking at the security standards discussed in section 5.2.2.2, security standards such as ISO27799, ISO27001, ISO27002 and MSS were found in the public hospital for the protection of ePHI. The results on policies indicated that some policies related to IT, HR, medicine and finance were existing in the public hospital. The findings showed that there were no established security policy pertaining to the security and protection of ePHI.

6.2.2 Security threats to ePHI in a public hospital

The second research objective aimed at assessing the security threats to ePHI in a public hospital. From the discussion in section 5.2.3, it was noted that cyber threats such as worm viruses, Trojan horses, shortcut viruses and technological threats such as power and system failure, network connection failure and outdated computers and operating system and outdated hospital system were experienced by participants in the public hospital. These threats cause hospital computers to unexpectedly shut down, crash and malfunction. According to Narayana et al (2010:203), such threats can potentially cause disruptions to hospital systems and ultimately lead to issues of public concern such as discrimination, embarrassment, identity theft, and loss of privacy, financial losses and economic harm. It was evident from the current findings that security threats encountered by participants in the public hospital are reported directly to the ICT department and hospital supervisors. Furthermore, these threats are reported to the security company which has been contracted by the hospital.

6.2.3 Security control measures to protect ePHI

In achieving the third objective which was to examine the security control measures used in the public hospital to prevent threats to and protect ePHI, it was necessary to interview hospital staff members to understand the security controls used in the public hospital and how effective and reliable they are. As noted above, three systems known as the PAAB system, Metro-file and RX were used in the public hospital to capture patient profile information, billing, and retrieving patients' files, dispatching medication and scheduling appointments. However, these systems were not integrated internally as they perform different functions and they were not integrated to other external systems outside the hospital. In the public hospital, administrative support staff were granted full permission access to ePHI captured in the PAAB and Metro-file system. However, the hospital restricts access to ePHI for IT staff, HR staff, finance staff and medical staff. Authentication and authorisation mechanisms were methods used in the public hospital to protect ePHI against access by unauthorised users. Mechanisms such as password and username were used in the public hospital to protect ePHI from unauthorised access, modification or disclosure. From

section 5.2.4.3 it was noted that defensive mechanisms such as the Windows firewall, antivirus program, and security audit log and data encryption were used in the public hospital to secure and protect ePHI against threats and risks. However, the antivirus program and firewall deployed in the public hospital were not updated. The effectiveness and reliability of these security controls were also investigated. The security controls used in the public hospital were perceived as reliable to consistently recognise any threats, as well as deal with them effectively.

6.2.4 Privacy issues associated with ePHI

The fourth objective of this study aimed at assessing privacy issues associated to ePHI about patients in the public hospital. Privacy-related issues can lead to serious complications for all patients involved. As a result, it was necessary to determine privacy issues that are most prominent in the public hospital. The findings on privacy issues confirmed that loss of patients' health data and unauthorised access to ePHI by hospital staff were major privacy issues encountered in the public hospital. It was noted from the study findings that loss of patients' health data and unauthorised access were resulting from unexpected power outages, inadequate backup system and sharing of login information (password and username) and hospital computers.

6.2.5 Recommended strategies for enhancing the security of ePHI

The last research objective of this study focused on obtaining strategies that could help to enhance and strengthen the security of ePHI in a public hospital. To do this, participants of this study suggested that it was necessary to improve hospital network connection and to upgrade hospital computers, the operating system and the PAAB system. It was emphasised that the public hospital should implement an appropriate backup, data recovery and biometric system, and update the antivirus and firewalls on a regular basis. Finally, the implementation of a security policy was proposed as another strategy that could improve the security and protection of ePHI.

6.3 Conclusions of the study

The conclusions of the study are based on the research objectives. According to Shuttleworth (2009:101), conclusions involve "summing up the paper and giving a very brief description of the results, although you should not go into too much detail about this" and that the conclusions "merely act as aid to memory" because anyone who reads a conclusion has essentially "read the entire" research report.

6.3.1 Policy and regulatory framework governing the security of ePHI

This study intended to analyse the policy and regulatory framework governing the security of ePHI in a public hospital in South Africa. It is emerged from the findings that the hospital comply with a number of legislation. However it can be concluded that some of the key legislation do not adequately address concerns relating to the security of ePHI. The study further concludes that pieces of legislation are useful to guide participants about the security and protection of ePHI in the public hospital.

The findings of this study revealed that the hospital has adopted a set of security standards such as ISO27799, ISO27001, ISO27002 and MSS standards. Therefore, it can be concluded that there is a clear gap of other ISO standards that should be adopted in the public hospital to strengthen the security of ePHI. The study findings indicated minimal policies that exist in the public hospital. It can be concluded that, despite the existing policies, the public hospital lacks a clear formal security policy that addresses the requirements for protecting ePHI. Therefore, the absence of security policy can negatively influence the security of ePHI in the public hospital. As a result, this situation could put the hospital at risk of suffering from unauthorised access and other breaches.

6.3.2 Security threats to ePHI

This study findings established that the public hospital faces a multitude of cyber threats such as worm viruses, Trojan horses, shortcut viruses and technological threats such as poor network, power and system failure, obsolete computers and operating system and outdated hospital system. The study further concludes that despite the hospital efforts to protect ePHI, existing security control measures are not effective enough to protect ePHI stored in the hospital systems.

6.3.3 Security control measures

This study discovered which security controls were used in the public hospital to protect ePHI against various threats. In line with the findings, it can be concluded that the public hospital uses three systems, which are not internally and externally integrated or linked. Based on the findings on access control, it can also be concluded that administrative support staff have access to ePHI, whereas IT staff, HR staff and finance staff members are restricted from accessing the system containing patients' information. The study findings revealed existing security controls that in place to protect ePHI in the public hospital, including encryption, antivirus, security audit log and the Windows firewall. However, it can therefore be concluded from this study that, despite the existing security controls, there is a need to constantly update the antivirus software and the Windows firewall to combat new viruses released. This situation could put hospital systems at risk of suffering from security threats, if the antivirus program and firewall are not updated against the most current viruses that have been released.

6.3.4 Privacy issues associated with ePHI

The study findings revealed that unauthorised access was experienced by participants in the public hospital. It is therefore the conclusion of the present study that sharing of passwords-usernames and computers among staff members causes unauthorised access to ePHI in the public hospital. Unauthorised access is regarded as a security loophole which can prove to be dangerous to hospital system, allowing hackers to access patient data by exploiting vulnerabilities in implementation. However, usage of the mentioned security measures such as password and username curbs this illicit activity by preventing exposure of patient data to unauthorised users. The general conclusion on privacy issues is that although the UPS battery has been installed in the hospital for data recover; however, unexpected power outage remains as the major challenge that leads to loss of patients' health data in public hospital.

6.3.5 Recommended strategies for enhancing the security of ePHI

The study findings showed that several strategies could be employed to in the public hospital to enhance the security of ePHI. Thus, it can be concluded that back-up and data recovery system need to be implemented in the hospital and the antivirus program and the Windows firewall should be updated regularly. It can also be concluded that hospital computers and operating system needs to be upgraded. Evidently, the hospital uses the old version of PAAB system which causes patients to wait. As a result, this study concludes that a new hospital system should be implemented in the public hospital. Based on the findings, this study further concludes that a biometric system should be implemented to restrict access to ePHI.

6.4 Recommendations

Recommendations are proffered based on the findings of the study, conclusions adduced above and the literature reviewed. These recommendations are essential for the hospital CEO, hospital managers and stakeholders to enhance the security of ePHI. The study recommends the following based on the study findings:

6.4.1 Policy and regulatory framework governing the security of ePHI

The public hospital should comply with other legislation that support the security, privacy, and integrity of sensitive healthcare data, such as the Electronic Communication and Transactions Act 25 of 2002 and National Credit Act 34 of 2005. These pieces of legislation address the protection of personal information obtained or collected from the public in South Africa. Adhering to other ISO standards such as, ISO27004, ISO27011 (privacy protection) and ISO17975 (privacy breach) is recommended for enhancing the protection and security of ePHI. In the absence of security policy in the public hospital, the study recommends the need to develop a clear, enforceable and comprehensive security policy with support of legislation regarding information security and emphases on protection and security of ePHI.

The security policy must be approved by hospital authorities as these are the cornerstones of the hospital and reviewed on a regular and consistent basis. The hospital managers should create guidelines for continuous review of the security policy to incorporate new threats, technological

and organisational changes. According to Cucoranu et al (2013:04), security policies are required to cover the security defensive mechanisms available in the hospital to provide individuals with access to hospital systems and ePHI. Furthermore, the hospital staff should be trained in the security policy after creation, together with relevant pieces of legislation governing the security of ePHI. This will expose staff members to legislation and policies governing patient records management.

6.4.2 Security threats to ePHI

In order to improve the security of ePHI, there is a need to upgrade hospital computers to resolve issues such as malfunction, error messages, poor performances and unexpected shutdown. The public hospital should consider purchasing newly advanced computers that run with Windows 8 or 10 professional edition and advanced Central Processing Unit (CPU) such as i5 or i7. This will enhance the speed and performance of hospital computers and avoid patients waiting for assistance. The public hospital should intensify and improve its network infrastructure to meet the expectation and requirements of hospital staff and patients. The 802.11 ac WI-FI network should be installed in the public hospital to provide high-speed bandwidth such as 5G. The 5G technology will enable the hospital network to operate in a stable and highly reliable way. Large hospitals like the public hospital require support for more sophisticated network connections, higher bandwidth and higher network performance.

6.4.3 Security control measures to protect ePHI

The study recommends the need to automate the updates of the Windows firewall to occur regularly to prevent outside access to hospital networks and to limit access to the outside from within the hospital network. The updated firewall can block unwanted or dangerous transmissions from unauthorised users and ensure that only appropriate PHI and personnel are allowed access to the hospital network. The study further recommends the use of an antivirus program that provides continuously updated protection against malware, viruses, and other code that attacks computers through web downloads, CDs, email, and flash drives. An updated antivirus and a good firewall are capable of detecting and protecting computers and networks against newly released viruses

that may attack ePHI through web downloads, email and flash drives. Continuous updates are essential for ensuring hospital systems to receive the best possible protection at any given time. Although the available antivirus and firewall are used in the public hospital to detect and remove attacks, they are not sufficient as new viruses and attacks are released each day. Therefore, the public hospital should implement an Intrusion Protection System (IPS). An IPS can detect and identify attacks that a firewall and antivirus cannot detect, for example DDoS attacks. Furthermore, an IPS provides protection which monitors hospital networks and systems for malicious activities. One advantage of this system is that it uses a set of predetermined rules to manage intrusions automatically or to alert security and IT staff to manually address events.

6.4.4 Privacy issues associated with ePHI

In order to avoid unauthorised access to ePHI in the public hospital, sharing of login credentials (password and username) should be prohibited. Hospital employees should avoid sharing their password and username with anyone, and they should always log off/out when leaving a terminal to avoid leaving ePHI visible to unauthorised personnel. The public hospital should prohibit the sharing of password-username among hospital employees. According to Cucoranu et al (2013:12), healthcare organisations should prohibit the sharing of login information to prevent unauthorised access to ePHI, and unauthorised alterations and loss of patient health data. Chen, Lo and Yeh (2012:101) emphasise that the utilisation of usernames and passwords is a traditional type of security technique to control access to ePHI in hospitals. However, these security techniques are becoming insufficient. Therefore, the hospital managers should consider moving to a higher level of security technology to improve the security of ePHI. A biometric system and RIFD system should be implemented to control and restrict access to ePHI.

According to Smith (2008:48), biometrics are unique and their use makes it very difficult, if not impossible, to forge identity. This system will prevent sharing of passwords-usernames among hospital employees, thereby reducing the risks of unauthorised access to ePHI. The public hospital should also consider using RFID tags to restrict access to ePHI. According to Shank, Willborn, PytlikZillig and Noel (2012:251), biometrics and RFID have the capacity to enhance the security of ePHI through restricting authorised access to a limited number of individuals. In order to

strengthen access control measures in the public hospital, an appropriate access control policy should be formulated to allow authorised hospital users to access ePHI in a timely manner.

Unplanned power/system outages can result in the sudden loss of patient data, therefore it is critical for healthcare organisations to develop robust defensive mechanisms that minimise loss of data and help to recover patient data. In order to minimise loss of patient health data in the public hospital due to unexpected outages, the study suggests the implementation of data protection mechanisms such as cloud-based backup system and data recovery systems. These systems will help to restore and back up patients' health data and hospital staff employees to recover data that were corrupted or deleted as a result of unexpected power outage or shutdown. Furthermore, hospital employees should be properly and regularly trained and equipped with new skills and competencies on how to use alternative methods or strategies to backup and recover ePHI in case of power outages or downtime.

6.5 Suggestions for future research

This study makes several important suggestions for additional future research in the areas of health information security. Several areas for future research include: security of big data in the healthcare sector, cyber-security in South African healthcare facilities, regulatory and compliance issues, privacy and security in the healthcare sector and security policy in healthcare information systems. The present study explored the security of ePHI in a public hospital. This study was limited to one public hospital in South Africa, its countermeasures and employees' experiences. Future research may be conducted across all spectra of hospital staff to find out which policies, security defensive mechanisms and security challenges are present in other South African hospitals. Conducting a research in more than one hospital will provide more precise conclusions and allow for more generalisability. Furthermore, this will help to obtain more scientific evidence to justify the findings of this study and develop practices to address multifaceted security threats and risks. Given the fact that the current study was conducted in a public hospital in the Gauteng province, future research may be carried out in private hospitals in South Africa.

Future research could pursue public hospitals in other provinces and eliciting information from different demographic groups could help provide much greater insight in the area and permit for much better generalisations. The present study was exploratory in nature, thus there is a need for future research to consider a comparative analysis or cross-sectional study between South Africa and other African countries to investigate their security strategies and practices to protect ePHI and to compare the findings. The study adopted a qualitative approach for the purpose of gaining deeper understanding of the phenomenon being studied. Therefore, future research should consider using a quantitative approach to target the larger population as the qualitative approach has its own limitations. Future research could also include both quantitative and qualitative approaches, which is a mixed method approach. This approach to inquiry could add value and provide deeper and broader insights into security of ePHI. Considering that there is no security policy that addresses the protection of ePHI in the public hospital, future research studies should be conducted to understand the content and context of healthcare security policy. Lastly, it is suggested that the theoretical models and frameworks related to privacy and security of ePHI should be developed and explored.

6.6 Implications of the study

The present study has wide implications for society, policy, practice and theory. In relation to society, the findings from this research study demonstrate values for South African society. The present study contributes towards improving scholarly information and increasing access and use of information that enhances research output. By addressing the issues related to the security and privacy in hospitals, the research output and quality are enhanced. The study further creates awareness among hospital patients about how their personal information should be protected. From the policy perspective, the findings of the present study have the capacity and potential to influence the formulation of security policy and procedures to help direct and guide on the security of ePHI. The findings revealed that the public hospital covered in this study did not have a security policy. Therefore, the findings of the present study are useful in providing policy direction to hospital managers, policymakers and professional bodies and this study may be useful in establishing national policy framework for supporting the security of ePHI in South African hospitals.

With regard to health practice, the study has meaningful implications for hospital managers, stakeholders and employees. Firstly, the present study contributes to practice by providing a detailed articulation of the actual state of security in the public hospital. The study contributes to health practice by foregrounding the need for IT staff, hospital managers and stakeholders in the hospital to provide and improve on existing defensive mechanisms to protect ePHI. The study also contributes to health practice by identifying some strategies for improving the security of ePHI in the hospital. The study provides a new research area that may be explored by scholars and researchers interested in the field of health information security especially from developing country such as South Africa where the understanding of security and privacy of ePHI is limited. The study provides the basis for IT professionals and hospital stakeholders to take the necessary measures to mitigate threats and risks.

The theoretical implications of the present study are that the existing literature reviewed indicated inadequate research studies on security of ePHI in private and public hospitals in South Africa. As a result, this study fills this gap and makes a discernible contribution to the existing body of scientific knowledge by being the first research study to explore the security of ePHI in South Africa. The literature reviewed did not reveal studies that indicate security frameworks being used towards the security of ePHI. Therefore, the present study has also generated scientific knowledge by proposing a conceptual framework (See figure 1.1) that encompasses a holistic approach towards the security of ePHI in hospitals. In addition to theoretical implications, this research developed a conceptual framework provides a systematic way of understanding the security of ePHI. In this study, the researcher did not apply any theory suitable for studying the population and the setting. However, the theoretical implications of this study is that, a conceptual framework was proposed and developed in this study which will serve as the basis for modifying existing theories.

6.7 Final conclusion

The present study out to explore the security of electronic personal health information in a public hospital in South Africa. The study was presented in five chapters, commencing with the introductory Chapter One, which provided the background of the study. The purpose of the study,

research objectives and the conceptual framework were also presented in this chapter. Chapter Two of the study was predominantly a literature review on security of ePHI. The third chapter described and explained research methodology used in the study to achieve the research objectives. Chapter Four analysed and presented the data gathered through semi-structured interviews, document analysis and systems analysis, and presented according to themes emerged from the findings. The final chapter, Chapter Five, presented the summary of findings, conclusions drawn from findings, recommendations based on the findings of the study, suggestions for future research and implications of the study.

The study was qualitative in nature and adopted the single case study design. A conceptual framework was developed to guide this study and facilitate an understanding of security of ePHI. The findings were also aligned with the research objectives and the literature review. It is clear from the findings that pieces of legislation (POPI Act, PAIA, PAJA, NH Act, NARSSA, Constitution of the RSA and GDoH PAIM Act) are in place to ensure the protection of ePHI. Findings indicated that security standards such as ISO27799, ISO27001, ISO27002 and MSS are adopted in the public hospital. It was discovered that the public hospitals lack a clear security policy. Security threats such as cyber threats and technological threats were among the most prevalent threats encountered in the public hospital. However, defensive security measures such as encryption, firewall, antivirus, and security audit log exist in the public hospital to protect ePHI against such threats. In conclusion, the security of ePHI is one of the key ethical values in the health field. Therefore, protecting and securing ePHI of patients are of the most important duties of healthcare organisations. Regulations, security policies and practices are at least as important as defensive mechanisms in protecting ePHI and patient privacy. Most importantly, healthcare organisations should upgrade the security of their information systems to protect ePHI stored in databases against unauthorised access, malicious codes and other cyber-attacks.

References

Abbas, KD. 2015. Knowledge management strategies and practices in Nigerian agricultural research institutes. Doctoral dissertation, University of KwaZulu-Natal, Pietermaritzburg, South Africa. Available from: https://researchspace.ukzn.ac.za/xmlui/handle/10413/12995 (Accessed 22 February 2017).

Abhang, TA & Kulkarni, UV. 2013. An integrated approach to detect and limit IP spoofing. *Journal of Computer Science and Information Technology* 2(7):59-65.

Abouzakhar, A. 2013. Critical infrastructure cyber security: a review of recent threats and violations. Paper presented at the 12th European Conference on Cyber Warfare and Security, Finland, 11–12 July 2013, 1-10.

Abouelmehdi, K, Beni-Hessane, A & Khaloufi, H. 2018. Big healthcare data: preserving security and privacy. *Journal of Big Data* 5(1): 1.

Adesina, AO, Agbele, KK, Februarie, R, Abidoye, AP & Nyongesa, HO. 2011. Ensuring the security and privacy of information in mobile health-care communication systems. *South African Journal of Science*, 107(9-10):27-33.

Akanbi, MO., Ocheke, AN., Agaba, PA., Daniyam, CA., Agaba, EI., Okeke, EN & Ukoli, CO. 2012. Use of electronic health records in sub-Saharan Africa: progress and challenges. *Journal of Medicine in the Tropics*, 14(1):1.

Akintoye, A. 2015. Developing theoretical and conceptual frameworks. Jedm.oauife.edu.ng>uploads>2017/03/07 (Accessed 2017 February 22).

Al Ameen, M, Liu, J & Kwak, K. 2012. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems* 36(1): 93-101.

Alban RF, Feldmar D, Gabbay, J & Lefor, AT. 2005. Internet security and privacy protection for the healthcare professional. *Current Surgery* 62: 106-10.

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L & Côté, I. 2015. A pattern-based and tool-supported risk analysis method compliant to ISO 27001 for cloud systems. *International Journal of Secure Software Engineering (IJSSE)*, *6*(1): 24-46.

Alshehri, S, Mishra, S & Raj, R. 2014. Insider threats and access control in e-Health*16th International Conference on e-Health Networking, Applications and Services. IEEE* 1(2):34-42.

Altamimi, AM. 2016. Security and privacy issues in e-Healthcare Systems: Towards Trusted Services. *International Journal of Advanced Computer Science and Applications* 7(9): 229.

American Academy of Paediatrics. 2010. Paediatric Practice Action Group and Task Force on Medical Informatics. 1999. Privacy protection of health information: patient rights and paediatrician responsibilities. *Paediatrics* 104(4): 973-977.

Anderson, C & Agarwal, R. 2011. The digitisation of healthcare: boundary risks, emotion and consumer willingness to disclose personal health information. *Information Systems Research* 22(3): 469-490.

Anderson, R, Barton, C, Boehme, R, Clayton, R, Van Eeten, MJG, Levi, M, Moore, T & Savage, S. 2012. Measuring the cost of cybercrime. Available from: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf. (Accessed 5 December 2012).

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.

Andriole, KP & Khorasani, R. 2010. Patient privacy and security of electronic medical information for radiologists: the basics. *Journal of the American College of Radiology* 7(3): 397-9.

Aselton, P & Affenito, S. 2014. Privacy issues with the electronic medical record. *Annals of Nursing and Practice* 1(2): 1-9

Asghar, MR, Lee, T, Baig, MM, Ullah, E., Russello, G & Dobbie, G. 2017. A review of privacy and consent management in healthcare: a focus on emerging data sources. *arXiv preprint arXiv:1711.00546*.

Asija, R & Nallusamy, R. 2014. A survey on security and privacy of healthcare data. Proceedings of the Third Annual Global Healthcare Conference, Singapore.

Asogwa, BE. 2012. The challenge of managing electronic records in developing countries: implications for records managers in sub-Saharan Africa. *Records Management Journal* 22(3): 198-221.

Ataguba, JE & McIntyre, D. 2012. Paying for and receiving benefits from health services in South Africa: is the health system equitable? *Health Policy and Planning* 27(1): 35-45.

Avancha, S, Baxi, A & Kotz, D. 2012. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)* 45(1): 3.

Ayatollahi, H & Shagerdi, G. 2017. Information security risk assessment in hospitals. *The Open Medical Informatics Journal* 11(3): 37.

Ball E, Chadwick, DW & Mundy, D. 2003. Patient privacy in electronic prescription transfer. *IEEE Secure Privacy* 1(2): 77-80.

Beaumont, R. 2011. Types of health information systems (IS). Available from: http://www.floppybunny.org/robin/web/virtualclassroom/chap12/s2/systems1.pdf(Accessed 12 December 2011).

Beck, EJ., Gill, W. & De Lay, PR. 2016. Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. *Global health action* 9(1):320.

Bell, G & Ebert, M. 2015. Healthcare and Cyber Security. Available from: https://advisory.kpmgus/content/dam/kpmgadvisory/PDFs/ManagementConsulting/2015/KPMG-2015Cyber-Healthcare-Surveypdf (Accessed 12 January 2015).

Benhard R, Grascher, F & Neubauer. 2008. Pseudonymization for improving the privacy in e-health applications. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* 2(3): 255-255.

Bergkvist S. 2015. *Health system in India: bridging the gap between current performance and potential*. New Delhi: National Institution for Transforming India Aayog.

Bey, JM & Magalhaes, JS. 2013. Electronic health records in an occupational health setting – Part II. A global overview. *Perspectives in International Occupational Health Nursing* 61(3): 95-98.

Bhaskar, SM & Ahson, SI. 2008. *Information Security: A practical Approach*. Oxford: Alfa Science International Ltd

Biswas, BC & Choudhuri, SK. 2012. Digital information resources for disaster management of Libraries and Information Centres. *Bangladesh Journal of Library and Information Science*, 2(1): 12–21. Available from: https://doi.org/10.3329/bjlis.v2i1.12915

Blake, L et al. 2017. Developing robust data management strategies for unprecedented challenges to healthcare information. *Journal of Leadership, Accountability and Ethics* 14(1): 22-31.

Blober, B., Nordberg, R., Bavis, JM & Pharow, P. 2006. Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8):597–623.

Braithwaite, J, Westerbrook, MT, Travaglia, JF, Iedema, R, Mallock, NA, Long, D, Nugus, P, Forsyth, R, Jorm, C & Pawsey, M. 2007. Are health systems changing in support of patient safety? A multi-methods evaluation of education, attitudes and practice. *International Journal of Healthcare Quality Assurance* 20(7): 585-601.

Brauch, HG. 2011. Concepts of security threats, challenges, vulnerabilities and risks. In Brauch, HG. et al. *Coping with global environmental change, disasters and security*. Springer-Verlag, Berlin, Heidelberg, 61-106.

Braun, V & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3:77–101.

Braun, V & Clarke, V. 2013. *Successful qualitative research: a practical guide for beginners*. London: SAGE.

Bridges, L. 2008. The changing face of malware. *Network Security* 2(1): 17-20.

Brink, H, Van der Walt, C & Rensenbury, G. 2012. *Fundamental of research methodology for healthcare professionals.* 3rd ed. Cape Town: Juta and Company.

Brodnik, M, Rinehart-Thompson, L & Reynolds, R. 2012. *Fundamentals of law for health informatics and information management professionals*. Chicago: AHIMA Press.

Brown-Podgorski, BL, Hilts, KE, Kash, BA, Schmit, CD & Vest, JR. 2018. The Association between State-Level Health Information Exchange Laws and Hospital Participation in Community Health Information Organisations. In *AMIA Annual Symposium Proceedings* (Vol. 2018, p. 313). American Medical Informatics Association.

Bryman, A. 2012. *Social research methods*. New York: Oxford University Press

Bryman, A. 2016. *Social research methods.* 5th ed. Oxford: Oxford University Press.

Burns, N & Grove, SK. 2011. *Understanding nursing research: building evidence based practice*. 5th ed. Philadelphia: Elsevier Saunders.

Buys, M. 2017. Protecting personal information: implications of the Protection of Personal Information (POPI) Act for healthcare professionals. *South African Medical Journal* 107(11): 954-956.

Byrne, E., Daykin, N & Coad, J. 2016. Participatory photography in qualitative research: A methodological review. *Visual Methodologies, 4*(2):1-12.

Cadick R. 2005. Protecting networked medical devices from worms and viruses. *Biomedical Instrumental Technology*.

Cadwlader, W & Taft, L. 2017. Wannacry Ransomware Attacks Should Be A Wake-Up Call for. Clients & Friends Memo, 1.

Canadian Institute for Health Information. 2016. Available from: https://www.cihi.ca/en/faq/what-is-personal-health-information (Accessed 28 August 2016).

Capelão, F & Barbosa, H. 2018. Cybersecurity in healthcare: risk analysis in health institution in Portugal. *International Journal for Research & Development in Technology* 9(3): 2349-3585.

Carro, SA & Scharcanski, J. 2006. A framework for medical visual information exchange on the web. *Computers in Biology and Medicine* 36(4): 327-338. Available from: https://eurekamag.com/pdf/011/011684930.pdf (Accessed 16 July 2018).

Carter, M. 2001. Integrated electronic health records and patient privacy: possible benefits but real dangers. *Medical Journal of Australia* 172(1):28–30.

Catwell, L & Sheikh, A. 2009. Evaluation of eHealth innovations: the need for continuous systemic evaluation. *PLoS Medicine* 6(8):1-6.

Cavalli, E, Mattasoglio, A, Pinciroli, F & Spaggiari, P. 2004. Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics* 73(3): 297-303.

Charles, D, Gabriel, M & Searcy, T. 2015. Adoption of EHR systems among US non-federal acute care hospitals, 2008–2014. *ONC Data Brief*, 23 April 2015:1-10.

Chauhan, K & Prasad, V. 2015. Distributed Denial of Service (DDos) attack techniques and prevention on cloud environment. *International Journal of Innovations & Advancement in Computer Science* 4: 210-215.

Cheung, E & Waldeck, A. 2016. Literature review. Literacy and reading in libraries (2011 – 2016). UIL Hamburg. Available from: http://www.tru.ca/_shared/assets/Literature_Review (Accessed 10 April 2016).

Chen, HM, Lo, JW & Yeh, CK. 2012. An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. *Journal Medical Systems* 36(6):3907-3915.

Chen, YY, Lu, JC, and Jan, JK. 2012. A secure EHR system based on hybrid clouds. *Journal of Medical Systems* 36(5):3375-3384.

Chhanabhai, P & Holt, A. 2007. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine* 9(1):8.

Chigada, J. 2015. Knowledge-management practices at selected banks in South Africa. Master's Dissertation, University of South Africa, Pretoria.

Chilisa, B & Preece, J. 2005. *Research methods for adult educators in Africa*. Hamburg: UNESCO institute of education.

Chilisa, B & Kawulich, BB. 2012. *Selecting a research approach: paradigm, methodology and methods.* In: *Doing social research, a global context*. London: McGraw Hill.

Chowles, T. HNFS identifies 42 health information systems in SA. E Health News, 25 June 2014. Available from: http://ehealthnews.co.za/hnsf-identifies-42-health-information-systems-sa/ (Accessed 17 July 2018).

Cilliers, L & Wright, G. 2017. Electronic health records in the cloud: improving primary healthcare delivery in South Africa. *Studies in Health Technology and Informatics* 245: 35-39.

Cipresso P, Gaggioli A, Serino S, Cipresso S & Riva G. 2012. How to create memorisable and strong passwords. *Journal for Medical Internet Research* (14): 10.

Clarke, V & Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist 26*(2):120-123.

Clem, A, Galwankar, S & Buck, G. 2003. Health implications of cyber-terrorism. *Prehospital and disaster medicine* 18(3): 272-275.

Cluley, G. 2010. Sizing up the malware threat-key malware trends for 2010. *Network security* (4): 8-10. Available from: http://dx.doi.org/10.1016/S1353-4858(10)70045-3(Accessed 23 May 2010).

Coleman, A. 2010. Developing an e-health framework through electronic healthcare readiness assessment. Master's Dissertation, Nelson Mandela Metropolitan University, South Africa.

Collier, R. 2014. New tools to improve safety of Electronic Health Records. *CMAJ* 186(4): 251-251.

Conaty-Buck, S. 2017. Cybersecurity and healthcare records. *American Nurse Today* 12(9): 62-64.

Connelly, LM. 2013. Demographic data in research studies. *Medical Surgery Nursing* 22(4): 269-271.

Connoway, LS & Powell, RR. 2010. *Basic research methods for librarians.* 5th ed. Santa Barbara, California: Libraries Unlimited.

Conrick, M & Newell, C. 2006 Issues of ethics and law. In M Conrick (Ed) *Health Informatics: transforming healthcare with technology* 320. Melbourne: Thomson Social Science Press.

Cooper, T & Collman, J. 2005. Managing information security and privacy in healthcare data mining. *Medical Informatics* 95-137.

Côrtes, PL & Côrtes, EGDP. 2011. Hospital information systems: a study of electronic patient records. *Journal of Information Systems and Technology Management* 8(1): 131-154.

Coventry L & Branley, D. 2018. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas* 113: 48-52.

Creswell, JW. 2009. *Research design: qualitative, quantitative and mixed methods approaches* 3rd ed. Los Angeles: Sage Publications Inc.

Creswell, JW. 2012. *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* 4th ed. Boston, MA: Pearson Education, Inc.

Creswell, JW. 2013. *Qualitative inquiry and research design: choosing among five approaches.* Kindle ed. Thousand Oaks, CA: SAGE.

Creswell, JW. 2014a. *Research design: qualitative, quantitative and mixed methods approach*. 4th ed. Thousand Oaks, CA: SAGE.

Crouch, S. 2013. Ensuring patient privacy in cyberspace. *Hospitals & Health Networks (H&HN) Daily*, 10 September 2013. Available from: http://www.perfectserve.com/wpcontent/uploads/2015/09/ensuring-patient-privacy-cyberspace.pdf (Accessed 16 July 2018).

Cucoranu, IC, Parwani, AV, West, AJ, Romero-Lauro, G, Nauman, K, Carter, AB, Balis, UJ, Tuthill, MJ & Pantanowitz, L. 2013. Privacy and security of patient data in the pathology laboratory. *Journal of pathology informatics* 4(1): 123-129.

Cyber-attacks reaching a critical point in SA. *SABC News*, 19 April 2017. Available from: http://www.timenews.co.za/timenews-sabc-news-cyber-attacks-reaching-acritical-point-in-sawednesday-19-april-2017 (Accessed 17 July 2018).

Cybercrime threatens healthcare in South Africa. 2016. *SABC News Africa*, 15 July 2016. Available from: http://www.itnewsafrica.com/2016/07/cybercrime-threatens-healthcare-sector-in-south-africa/ (Accessed 17 July 2018).

Daglish, D & Archer, N. 2009. Electronic personal health record systems: a brief review of privacy, security, and architectural issues. In *World Congress on Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09,* 110-120.

Data Protection Laws of the World. 2017. DLA Piper. Available from: http://www.dlapiperdataprotection.com (Accessed 2017 December 2017).

Davidson, MA. 2005. A matter of degrees. *Security Management* 49(12): 72-99.

Dawson, C. 2009. *Introduction to research methods*. Oxford: How to Books.

De Bruyn, M. 2014. The Protection of Personal Information (POPI) Act: impact on South Africa. *International Business & Economics Research Journal* 13(6). Available from: http://search.proquest.com/opview/4ee18ed87793b12df7346b50a25c0a1d/1?pqorigsite=gscholar (Accessed 16 July 2018).

Denning, DE. 2000. Statement of Dorothy E. Denning (2000), available from: www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm. (Accessed 17 July 2012).

Denning, DE. 2012. *Policing cyber hate, cyber threats and cyber terrorism*. Imran, A. & Brian, A. (editors) Burlington: Ashgate Publishing Company.

Denscombe, M. 2007. *The good research guide for small-scale social research projects*. 3rd ed. Maidenhead: Open Press University.

Denscombe, M. 2010. *The good research guide: for small-scale social research projects*. 4th ed. Maidenhead: Open University Press.

De Villiers, JT. 2006. The knowledge and skills gap of medical practitioners delivering district hospital services in the Western Cape, South Africa. *South African Family Practice* 48(2): 16-16.

Department of Health (South Africa). 2007. *First Draft White Paper on E-Health*. Available from: http://www.doh.gov.za (Accessed 28 May 2013).

Department of Health (South Africa). 2008. *Republic of South Africa Electronic Health Record for South Africa*. Available from: http://southafrica.usembassy.gov/root/pdfs/pepfarhmis-docs/ndoh-e-hr-for-south-africa.pdf (Accessed 27 October 2012).

Department of Health (South Africa). 2012. *National e-Health Strategy, South Africa, 2012–2017.* Pretoria: Department of Health.

Department of Health and Human Services (United States). 2014. *Health information privacy*. Available from: http://www.hhs.gov/ocr/privacy (Accessed 28 August 2014).

Department of Health and Human Services (United States). Office of the Secretary. 2003. Code of Federal Regulations (CFR). Part II. 45 CFR. Part 160, 162 & 164, Health Insurance Reform: Security Standards. Final Rule. *Federal Register*, 68(34): 8333–8381.

Department of Health and Human Services (United States). Office for Civil Rights. 2013. *Omnibus HIPAA, Rulemaking.* Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html (Accessed 17 July 2018).

Dickinson, G, Fischetti, L & Heard, S. 2004. HL7 EHR System Functional Model Draft Standard for Trial Use. *Health Level, 7*. Available from: http://www.hl7.org/documentcenter/public_temp_3ED3F1F3-1C23-BA17 0C917DF4550202DD/wg/ehr/HL7_EHR-S_DSTU.pdf (Accessed 15 May 2010).

Dimitriou, T & Loannis, K. 2008. Security issues in biomedical wireless sensor networks. In *Proceedings of the First International Symposium on Applied Sciences on Biomedical and Communication Technologies* (ISABEL), Aalborg, Denmark, 25-28 October 2008.

Ducom, JC, Topol, EJ & Steinhubl, SR. 2016. Privacy and security in the era of digital health: what should translational researchers know and do about it? *American Journal of Translation Research*, 8(3): 1560-1580. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4859641/ (Accessed 19 February 2018).

Duncan, AJ, Creese, S & Goldsmith, M. 2012. Insider attacks in cloud computing. In Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). *IEEE* 2(3): 857-862.

Du Plooy-Cilliers, F, Davis, C & Bezuidenhout, R. 2014. *Research matters*. Cape Town: Juta.

Edmonds, WA & Kennedy, TD. 2013. *An applied reference guide to research designs: quantitative, qualitative and mixed methods*. California: Sage Publications.

Ekelhart, A, Fenz, S & Neubauer, TH. 2009. *AURUM: a framework for information security risk management. Hawaii: TUM University*. In Proceedings of the 42nd Hawaii International Conference on System Sciences, 1-10.

Electronic Communication Transaction Act (ECTA) (25 0f 2002). Vol.446 Government Gazette, Cape Town 2 August 2002.

Eling, M & Schnell, W. 2016. What do we know about cyber risk and cyber insurance? *The Journal of Risk Finance* 17(5): 1526-5943.

Elleithy, KM, Cheng, W & Sideleau, P. 2005. Denial of service attack techniques: analysis, implementation and comparison. *Journal of Systemic, Cybernetics, and Informatics* 3(1): 66-71.

Engebretson, P. 2011. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.

Evans, M, Maglaras, LA & Jaicke, J. 2016. Human behaviour as an aspect of cyber security assurance. arXiv preprint arXiv: 1601.03921

Eyisi, D. 2016. The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education curriculum. *Journal of Education and Practice* 7(15): 91-100.

Farzandipour M, Ahmady M, Sadoghi F & Karimi I. 2008. A comparative study on security requirements of electronic health records in selected countries. *Health System Research* 2(5): 139-149

Farzandipour, M, Sadough, IF, Ahmadi, M & Karimi, I. 2010. Security requirements and solutions in electronic health records: lessons learned from a comparative study. *Journal of Medical Systems* 34(4): 629-2.

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. Available from: https://www.sciencedirect.com/science/article/pii/S1532046412001864?via%3Dihub (Accessed 17 July 2018).

Ferreira A, Cruz-Correia R, Chadwick DW & Antunes L. 2007. Access control: how can it improve patients' healthcare. *Studies in Health Technology and Informatics* 12(7): 65-76.

Ferrier International. 2011. "Business against Crime South Africa on the Latest Crime Statistics". Available from: http://ferrierinternational.com/business-against-crimesouth-africa-on-the-latest-crime-statistics/ (Accessed 5 March 2011).

Fibikova, L & Mueller, R. 2012. Threats, risks and the derived information security strategy. In Reimer H, Pohlmann N & Schneider W *Securing electronic business processes: highlights*

of the Information Security Solutions Europe 2012 Conference, edited by. Wiesbaden: Springer, 11–20.

Flick, U. 2007. *Designing qualitative research*. London: Sage publication.

Fiza, AR, Lizawati, S, Zuraini, I & Narayana, SG. 2016. Safety and privacy issues of electronic medical records. *Indian Journal of Science and Technology* 9(42): 1-6.

Fuchs, L, Pernul, G & Sandhu, R. 2011. Roles in information security – a survey and classification of the research area. *Computers & Security* 30: 748-769.

Fulford, H & Doherty, N. 2003. Application of information security policies in Large UK Based organisations: An Exploratory Investigation. *Information Management and Computer Security* 11(3): 106-114

Gagneja, KK. 2017. Knowing the ransomware and building defense against it – specific to healthcare institutes. In Third International Conference on Mobile and Secure Services (MobiSecServ), 11-12 Feb, New Orleans. *IEEE* 1-5.

Goldman, J. 1998. Protecting Privacy to Improve Healthcare. 17 *Health Affairs.* 17(6): 47-60.

Gomes, R & Lapão, LV. 2008. The adoption of IT security standards in a healthcare environment. *Studies in Health Technology and Informatics* 13(6):765.

Gordon, WJ, Fairhall, A &Landman, A., 2017. Threats to information security – public health implications. *New England Journal of Medicine* 377(8): 707-709.

Grazioli, AM & Jarvenpa, J. 2013. *Information about phishing methods*. New York: Harper Collins.

Grimes, RA. 2001. *Malicious mobile code-virus protection for windows.* O'Reilly Media Inc. Sebastopol, CA

Gritzalis, D. & Lambrinoudakis, C. 2004. A security architecture for interconnecting information systems. *International Journal of Medical Informatics* 2(3):730.

Grove, SK., Burns, N & Gray, JR. 2013. *The practice of nursing research: appraisal, synthesis, and generation of evidence*. St. Louis.

Habib, MM, Pathik, BB & Maryam, H. 2014. *Research methodology – contemporary practices: guidelines for academic researchers.* Cambridge: Cambridge Scholars.

Harman, LB., Flite, CA & Bond, K. 2012. Electronic Health Records: privacy, confidentiality and security. *Virtual Mentor*, 14(9):712–719. Available from: https://www.ncbi.nlm.nih.gov/pubmed/23351350 (Accessed 17 July 2018).

Hassidim, A, Korach, T, Shreberk-Hassidim, R, Thomaidou, E., Uzefovsky, F, Ayal, S & Ariely, D. 2017. Prevalence of sharing access credentials in electronic medical records. *Healthcare Informatics Research* 23(3):176-182.

Hau D. 2003. *Unauthorised access- threats, risk and control*. GSEC Practical Assignment, Version 1.4b, Option 1, July 11, 2003

Health Insurance Portability and Accountability Act, 2015. Personal Identifiable Information in healthcare.

Health Professions Council of South Africa (HPCSA). 2008. *Guidelines for good practice in the healthcare professions. Booklet 10, Confidentiality: protecting and providing information*. Pretoria: HPCA.

Hedges, C & Williams, B. 2014. *Anatomy of research for nurses*. Sigma Theta Tau.

Henning, E., Van Rensburg, W & Smit, B. 2004. Finding your way in qualitative research.

Hennink, M, Hutter, I & Bailey, A. 2011. *Qualitative research methods*. London: Sage Publications.

Hesse-Biber, SN. 2010. *Mixed methods research: merging theory with practice.* New York: The Guilford Press.

HIPAA General Information. 2015. Available from: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/ (Accessed 12 September 2016).

Howell, KE. 2013. *Introduction to the philosophy of methodology*. London: Sage Publications

Huda, MN, Sonehara, N & Yamada, S. 2009. A privacy management architecture for patient-controlled personal health record system. *Journal of Engineering Science and Technology 4*(2): 154-170.

Institute, Software Engineering. 2013. The CERT Insider Threat Center. Available from http://www.cert.org/insider_threat/(Accessed 13 March 2014).

Ives, TE. 2014. The new 'e-clinician' guide to compliance. *Audiology Today* 26(1): 52-53.

International Organisation 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 17 July 2018).

International Organisation for Standardization. 2004. ISO/IEC Directives Part 2:2004 (Rules for the Structure and Drafting of International Standards). Available from:

http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/International%20Standardization/ISO/ISOIECDirectivesPart2pdfformat.pdf. (Accessed 10 December 2017).

IT News, Africa. 2016. Cybercrime threatens healthcare in South Africa. Available from: http://www.itnewsafrica.com/2016/07/cybercrime-threatens-healthcare-sector-in-south-africa/(Accessed 02 June 2019).

Jalali, MS & Kaiser, JP. 2018. Cybersecurity in hospitals: a systematic, organisational perspective. *Journal of medical Internet research* 20(5): 10-59.

James, E & Slater, T. 2014. Are you ready to write your methodology? In *Writing your doctoral dissertation or thesis faster*. London: SAGE Publications Ltd: 111-123.

Jannetti, MC. 2014. Safeguarding patient information in electronic health records. *AORN Journal*. 100(3): 7-8.

Jonker, J & Pennink, B. 2010. *The essence of research methodology: a concise guide for master and PhD students in management science*. Springer Science & Business Media**.**

Kahn, T. 2011. Government paves the way for move to paperless hospitals. Health Systems Trust. Available from: http://wwqw.hst.org.za/news/government-paves-way-move-paperlesshospitals (Accessed 14 May 2014)

Katuu SA. 2015. *Managing records in South African public healthcare institutions – a critical analysis.* PhD thesis. University of South Africa, Pretoria.

Katzenbeisser, S & Petkovic, M. 2008. *Privacy preserving recommendation systems for consumer healthcare services. In 2008 Third International Conference on Availability, Reliability and Security* 889-895.

Keen, J, Calinescu, R, Paige, R & Rooksby, J. 2013. Big data + politics = open data: The case of healthcare data in England. *Policy & Internet* 5(2): 228-243. Available from: http://doi.wiley.com/10.1002/1944-2866.POI330

Khalifehsoltani, SN & Gerami, MR. 2010. E-health challenges, opportunities and experiences of developing countries. In e-Education, e-Business, e-Management, and eLearning, 2010. IC4E'10. *International Conference on* (pp. 264-268). IEEE.

Khan, SI & Hoque, AS. 2015. *Towards development of health data warehouse: Bangladesh perspective*. International Conference on Electrical Engineering and Information

Communication Technology (ICEEICT), Dhaka, Bangladesh, 21–23 May 2015). Available from: https://ieeexplore.ieee.org/document/7307514/ (Accessed 17 July 2018).

Kim, KK, McGraw, Mamo, L & Ohno-Machado, L. 2013. Development of a privacy and security policy framework for a multistate comparative effectiveness research network. *Medical Care* 51: 66-72.

Knapp, KJ & Ferrante, CJ. 2012. Policy awareness, enforcement, and maintenance: critical to information security effectiveness in organisations. *Journal of Management Policy & Practice* 13(5): 66-80. Available from: http://www.nabusinesspress.com/jmppopen.html.

Kothari, CR. 2010. *Research methodology*. New Delhi, kk Grupta of new age international.

Kruse CS, Frederick B, Jacobson T & Monticone D. 2017a. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technology and Healthcare* 25(1): 1-10.

Kruse, CS, Smith, B, Vanderlinden, H & Nealand, A. 2017b. Security techniques for the electronic health records. *Journal of Medical Systems* 41(8): 127.

KPMG, S. 2017. *KPMG's Global Automotive Executive Survey on cyber threats in healthcare*. KPMG.

Kwon J & Johnson ME. 2013. Security practices and regulatory compliance in the healthcare industry. *Journal of American Medical Information Association* (20): 44-51.

Lafky, D & Horan, T. 2011. Personal health records: consumer attitudes toward privacy and security of their personal health information. *Health Informatics Journal* 17(1):63–71.

Landman, WA, Mouton, J & Nevhutalu, KH. 2000. *Chris Hani Baragwanath Hospital Ethics Audit.* Ethics Institute of South Africa. Available from: https://www.tei.org.za/phocadownloadpap/Research_Reports/CHBHFinalReport.pdf (Accessed 17 July 2018).

Lapan, SD, Quartaroli, MT & Riemer, FJ. 2012. *Qualitative research: an introduction to methods and designs*. San Francisco, CA: Jossey-Bass.

Lee, Y & Kozar, KA. 2005. Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM* 48(8):72-77.

Lee, WB & Lee, CD. 2008. A cryptographic key management solution for HIPAA privacy/security regulations. *Information Technology in Biomedicine, IEEE Transactions On* 12(1):34-41.

Lee, T, Chang, I, Lin, T & Wang, C. 2013. Secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. *Journal of Medical Systems* 37(3):9941-9948. Available from:https://link.springer.com/article/10.1007%2Fs10916-013-9941-8 (Accessed 17 July 2018).

Leedy, PD. 2005. *Practical research: planning and design.* 8th ed. Upper Saddle River, NJ: Pearson Education.

Lemke, J. 2013. Storage and security of personal health information. *Ontario Occupational Health Nurses Association Journal* 32(1):25-26.

Lichtman, M.2013. *Qualitative research in education: a user's guide*. 3rd ed. Thousand Oaks: SAGE Publications.

Litho, PK. 2010. ICTs and health in Uganda: benefits, challenges and contradictions. Available from: https://www.genderit.org/es/node/2201 (Accessed 17 July 2018).

Lin, B & Clark, L.1994. Information control and security policy in healthcare information systems. *Journal of International Information Management* 3(2): 2.

Lo-Biondo Wood, G & Haber, J. 2017. *Nursing research: methods and critical appraisal for evidence based practice*. 9th ed. St Louis: Elsevier.

Liu, V, Musen, A & Hou, T. 2015. Data breaches of protected health information in the United States. Journal of the American *Medical Association* 313(14): 14710-1473. doi:10.1001/jama.2015.2252

Lu, Y & Sinnott, RO. 2017. Semantic privacy-preserving framework for electronic health record linkage. *Telematics and Informatics* 35(4): 737-752.

Luna, R., Emily, R, Matthew, M, Sullivan, R & Clemens, K. 2016. Cyber threats to health information systems: a systematic review. *Technology and Healthcare* 24:1-9.

Luthuli, LP & Kalusopa, T. 2017. The management of medical records in the context of service delivery in the public sector in KwaZulu-Natal, South Africa: the case of Ngwelezana hospital. *South African Journal of Libraries and Information Science* 83(2): 2-10.

Madill, A & Gough, B. 2008. Qualitative research and its place in psychological science. *Psychological Methods* 13(3):254-271. Available from: https://www.academia.edu/2326112/M

dill_A._Gough_B._2008_Qualitative_research_and_its_place_in_psychological_science?auto=download (Accessed 17 July 2018).

Madsen, AK. 2013. Virtual acts of balance: virtual technologies of knowledge management as co-produced by social intentions and technical limitations. *Electronic Journal of E-Government* 11:183-197. Available from: http://www.ejeg.com/main.html (Accessed 12 November 2013).

Magnusson, RS. 2017. Framework legislation for non-communicable diseases: and for the Sustainable Development Goals? *BMJ global health* 2(3): 385.

Mahmood, AK. 2010. Information security management of healthcare system: case study of Blekinge Region Healthcare. Master's Thesis in Computer Science, Blekinge Institute of Technology.

Mair F, May, C & Murray E et al. 2009. Understanding the implementation and integration of e-Health services. Available from: http://www.netscc.ac.uk/hsdr/files/project/SDO_FR_08-1602-135_V01.pdf (accessed 2016-09-21)

Makhubela, SS. 2017. Knowledge retention at a platinum mine in North West Province of South Africa. Master's dissertation, University of South Africa, Pretoria.

Makulilo, AB. 2012. Privacy and data protection in Africa: a state of the art. *International Data Privacy Law* 2(3): 163-178.

Mansfield-Devine, S. 2016. Ransomware: taking businesses hostage. *Network Security,* 8–17, Available from: http://dx.doi.org/10.1016/S1353-4858(16)30096-4

Marutha, NS. 2011. *Records management in support of service delivery in the public health sector of the Limpopo province in South Africa*. Master's dissertation, University of South Africa, Pretoria.

Mchunu, NN. 2012. Adequacy of healthcare information systems to support data quality in the public healthcare sector, in the Western Cape, South Africa. Doctoral dissertation, Cape Peninsula University of technology.

McWay, D. 2010. *Legal and ethical aspects of health information.* 3rd ed. New York: Cengage Learning. Chapter 9.

Mars, M & Seebregts, C. 2008. Country case study for e-Health South Africa. Available from: https://www.k4health.org/sites/default/files/County%20Case%20Study%20for%20eHealth%20South%20Africa.pdf (Accessed 17 July 2018).

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

Marutha, NS. 2016. *A framework to embed medical records management into the healthcare service delivery in Limpopo Province of South Africa*. PhD Thesis, University of South Africa.

Marutha, N. 2018. The application of legislative frameworks for the management of medical records in Limpopo Province, South Africa. *Information Development*, p.0266666918772006.

Marutha, NS & Ngulube, P. 2010. *Records management: a foundation for business success, compliance and accountability with special focus on the public sector*. Paper presented at the Records Keeping and Data Management Conference, Johannesburg.

Maxfield, D & Latham, B. 2014. Data breaches: Perspectives from both sides of the wall. *South Carolina Lawyer* 25(6):28-35.

Maxwell, JC. 2012. *A treatise on electricity and magnetism*. Vol. 2. London: Forgotten Books.

Mayoh, J & Onwuegbuzie, AJ. 2015. Towards a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research* 9(1):91-107.

McCann, E. 2013. Kaiser reports second fall data breach. *Healthcare IT News*, 26 November 2013. Available from: https://www.healthcareitnews.com/news/kaiser-reports-second-fall-data-breach (Accessed 17 July 2018).

McGregor, SLT & Murnane, JA. 2010. Paradigm, methodology and method: intellectual integrity in consumer scholarship. *International Journal of Consumer Studies* 34(4): 419-427.

Mehraeen, S. 2012. Information security in hospital information systems in Beheshti and Tehran University of Medical Sciences. Doctoral thesis, Tehran University of Medical Sciences.

Mehraeen E, Ayatollahi H & Ahmadi, MA. 2013. Study of information security in hospital information systems. *Health Information Management* 10(6): 779-788.

Mehraeen, E, Ayatollahi, H & Ahmadi, M. 2016. Health information security in hospitals: the application of security safeguards. *Acta Informatica Medical* 24(1): 47-50

Mei, H, Dawei, J, Guoliang, L & Yuan, Z. 2009. Supporting database applications as a service. *In Proceedings of the 25th IEEE International Conference on Data Engineering*, 832-843.

Meingast, M, Roosta, T & Sastry, S. 2006. Security and privacy issues with healthcare information technology. *In 28th Annual Conference in Engineering in Medicine and Biology Society. EMBS'06*. *IEEE*, 5453-5458.

Meredith, B. 2005. Data protection and freedom of information. *British Medical Journal* 330(7490): 490-491. Available from: http://www.bmj.com (Accessed 8 March 2006).

Merisalo, LJ. 2015. Protecting patient identity: top three tips to combat heightened medical identify threat. *Healthcare Registration* 24(10):10-12.

Miles, MB, Huberman, AM & Saldana, J. 2013. *Qualitative data analysis: a methods sourcebook*. Thousand Oaks, CA: SAGE.

Millar, S. 2011. A cyber security risk assessment of hospital infrastructure including TLS/SSL and other threats. *Management* 2(7): 5.

Milošević, N. 2013. History of malware. *arXiv preprint arXiv:1302.5392*.

Moran C. 2009 Hospital district fires 16 over privacy violation. *Houston Chronicle*. Available from: www.chron.com/disp/story.mpl/hotstories/6738856.html(Accessed 2 March 2011).

M.Prem Inc. 2016. Practical challenges of complying with POPI. Available from: http://mprem.co.za/Publications/post/practical-challenges-of-complyingwith-popi(Accessed on May 2016).

Muaz, JM.2013. Practical guidelines for conducting research. Available from: http://www.enterprisedevelopment.org/wpcontent/uploads/150703_DCED_Guidelines on_good_research_MJ.pdf (Accessed 10 June 2015).

Mugo, DM & Nzuki, D. 2014. Determinants of electronic health in developing countries. *International Journal of Arts and Commerce* 3(3):49-59.

Mulligan, EC. 2001. Confidentiality in health records: evidence of current performance from a population survey in South Australia. *Medical Journal of Australia* 174(12):637-40.

Murchison, J. 2010. *Ethnography essentials: designing, conducting, and presenting your research*. San Francisco: John Wiley and Son.

Myers, MD. 2013. *Qualitative research in business and management*. Sage.

Narayana Samy, G, Ahmad, R & Ismail, Z. 2010. Security threats categories in healthcare information systems. *Health Informatics Journal* 16(3):201-209.

National Academy Press. 1997. Available from: https://www.nap.edu/ (Accessed 17 July 2018).

National Research Council (United States). 1997. *For the record: protecting electronic health information*. Washington: National Academy Press.

New South Wales Government. 2014. Health Records and Information Privacy Act, No. 71 O.D. 2002. Available from: https://www.legislation.nsw.gov.au/inforce/4ace6d6d-5d22-4e89-a1b5-45cb39ba6cef/2002-71.pdf (Accessed 12 October 2014).

Ngoepe, M. 2008. An exploration of records management trends in the South African public sector: a case study of the Department of Provincial and Local Government. Master's thesis. University of South Africa.

Ngoepe, M, Mokoena, L & Ngulube, P. 2010. Security, ethics and privacy in electronic records management in the South African public sector. *ESARBICA Journal* 29: 36-66.

Ngulube, P. 2000. Professionalism and ethics in records management in the public sector in Zimbabwe. *Records Management Journal* 10(3):161-173.

Ngulube, P. 2015. Trends in research methodological procedures used in knowledge management studies (2009 – 2013). *African Journal of Library, Archives and Information Science* 24(2) (forthcoming).

Ngulube, P, Mathipa, ER & Gumbo, MT. 2015. Theoretical and conceptual framework in the social sciences. In ER Mathipa & MT Gumbo (Eds.) *Addressing research challenges: making headway for developing researchers*. Mosala-MASEDI Publishers & Booksellers, 43-66.

Ngulube, P. 2020. Theory and theorizing. In P. Ngulube (ed.), *Handbook of Research on Connecting Research Methods for Information Science Research.* Hershey, PA: IGI Global

NHS CfH .2010. *Introduction to ISO 27000*. Available from:URL:http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards/iso (Accessed 15 June 2010).

Nieswiadomy, RM. 2012. *Foundations of nursing research*. (6th ed) Boston: Pearson Education.

Norton South Africa. 2012. *Norton cybercrime report, 2012*. Available from: http://za.norton.com/cybercrimereport/promo?inid=uk_hho_downloads_home_link_cybercrimereport (Accessed 17 July 2018).

NZPA. 1993. Privacy act 1993. New Zealand legislature, Public Act 1993 No. 28. (Accessed 17 May 2013). Available from: Available from:

http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html#whole (Accessed 25 December 2008).

Office for Civil Rights. 2008. "HIPAA privacy rule. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ index.html (Accessed 25 December 2008).

Ofulla, AV. 2013. *The secrets of hidden knowledge: how understanding things in the physical realm nurtures life*. Bloomington: Abbott Press.

Ohno-Machadoa, L, Silveira, PSP & Vinterbo, S. 2004. Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *International Journal of Medical Informatics* 73(7-9): 599-606.

O'Mahony, D, Wright, G, Yogeswaran, P & Govere, F. 2014. Knowledge and attitudes of nurses in community health centres about electronic medical records. *Curationis* 37(1):1-6.

Onuiri, E, Idowu, S & Oyindolapo, K. 2015. Electronic *health record systems and cyber security challenges*. In International Conference on African Development Issues 2015: Information and Communication Technology Track. Available from: http://eprints.covenantuniversity.edu.ng/5326/1/Paper%2054.pdf (Accessed 16 February 2016).

Onwuegbuzie, JA, Leech, LN & Collins, TMK. 2012. Qualitative analysis techniques for the review of the literature. *The Qualitative Report* 17(3): 1-28. Available from: http://www.nova.edu/ssss/QR/ (Accessed 2 June 2012)

Oosthuizen, H & Verschoor, T. 2008. Ethical principles becoming statutory requirements'. *SA Family Practice* 36 at 38 and A Gray, Y Vawda and C Jack 'Health policy and legislation: legislation and financing' (2012/2013) *South African Health Review* at 10 and 11.

Pankomera, R & Van Greunen, D. 2017. Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries. In *IST-Africa Week Conference (IST-Africa)* 3(2):1-11.

Papoutsi, 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 16 July 2018).

Parker, AMS. 2010. Cyberterrorism: An examination of the preparedness of North Carolina local law enforcement. *Security Journal* 23(3):159-173.

Partala, J., Keräneny, N., Särestöniemi, M., Hämäläinen, M., Iinatti, J., Jämsä, T., Reponen, J. & Seppänen, T. 2013. Security threats against the transmission chain of a medical health monitoring system. *In 15th International Conference on e-Health Networking, Applications & Services (Healthcom)* 243-248.

Pasquale, F. 2013. Grand bargains for big data: the emerging law of health information. *Maryland Law Review* 72(3): 682-772.

Patil, HK & Seshadri, R. 2014. Big data security and privacy issues in healthcare. *In Big Data (Big Data Congress), IEEE International Congress on* 762-765.

Pawar, MV & Anuradha, J. 2015. Network security and types of attacks in network. *Procedia Computer Science* 48: 503-506.

Peikari, HR, Ramayah, T, Shah, MH & Lo, MC. 2018. Patients' perception of the information security management in health centers: the role of organisational and human factors. *BMC Medical Informatics and Decision Making* 18(1): 102.

Pickard, AJ. 2013. Research method in information science. In AJ Pickard (Ed.), *Research method in information science*. 2nd ed. London: Facet.

Pisto, L. 2013. The need for privacy-centric role-based access to electronic health records. *Journal of Health and Life Sciences Law* 7(1): 79-112.

Polit, DF & Beck, CT. 2016. *Nursing research: generating and assessing evidence for nursing practice*. 10th ed. Philadelphia: Lippincott, Williams & Wilkins.

Pollits, MM. 2012. *Cyber terrorism fact and fancy.* Washington, DC: FBI Laboratory.

Ponemon Institute. 2012. *Third annual benchmark study on patient privacy & data security*. Available from: https://www.ponemon.org/local/upload/file/Third_Annual_Study_Patient_Privacy_FINAL.pdf (Accessed 17 July 2018).

Ponemon Institute. L. 2013. *Cost of data breach study: global analysis.* Poneomon Institute sponsored by Symantec.

Ponemon Institute. 2016. *Sixth annual benchmark study on privacy & security of healthcare data*. Available from: https://www.ponemon.org/library/sixth-annual- benchmark-study-on-privacy-security-of-healthcare-data-1 (Accessed 19 February 2018).

Ponemon Institute. 2017. Cost of Data breach Study: United State. Available at: https://ponemon.org/library/2017-cost-0f-data-breach-study-united-states. (Accessed on 19 March 2018)

Popoola, SI., Ojewande, SO., Sweetwilliams, FO., John, SN & Atayero, AA. 2017. *Ransomware: Current Trend, Challenges, and Research Directions*. London

Presidential National Commission on Information Society and Development (PNC). 2006. *e-Health*. [Online] available from: http://www.pnc.gov.za//index.php?option=com_contentandtask=viewandid=92andItemid=70 (Accessed 13 August 2007).

Punch, KF. 2013. *Introduction to social research: quantitative and qualitative approaches*. California: Sage Publications.

Purcell, JE. 2007. *Security control types and operational security*. Retrieved from World Wide Web.

Rajasekar, S, Philominathan, P & Chimnathambi, V. 2013. *Research methodology*. Available from: http://arxiv.org/pdf/physics/0601009 (Accessed June 12 2015).

Raman, A. 2007. Enforcing privacy through security in remote patient monitoring ecosystems. *6th International Special Topic Conference on Information Technology Applications in Biomedicine* 4(3):298-301.

Ramli, R, Zakaria, N & Sumari, P. 2010. Privacy issues in pervasive healthcare monitoring system: a review. *World Academy of Science Engineering and Technology* 7(2): 741-747.

Rana, ME, Kubbo & Jayabalan, M. 2017. Privacy and security challenges towards cloud-based access control. *Asian. Journal of Information Technology* 16(2-5): 274-281.

Rehman, A. 2014. Importance and measures of disaster management in libraries. *European Scientific Journal* 10(10): 319-325.

Republic of South Africa. 2000. Promotion of Access to Information Act, No. 2 of 2000. *Government Gazette,* 16(20852). Available from:https://www.saica.co.za/Portals/0/Technical/LegalAndGovernance/Promotion%20o

f%20Access%20to%20Inf mation%20Act%202%20of%202000.pdf (Accessed 17 July 2018).

Republic of South Africa. 2003. National Health Act, No. 61 of 2003. Available from: http://www.hst.org.za/uploads/files/chap2_03.pdf (Accessed 15 August 2015)Republic of South Africa. 2013. Protection of Personal Information Act, No. 4 of 2013. *Government Gazette*, 581(37067), 26 November 2013. Available from:https://www.gov.za/sites/default/files/37067_2611_Act4of2013ProtectionOfPersonalInfor_correct.pdf (Accessed 17 July 2018).

Riege, AM. 2003. Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative market research: An international journal* 6(2):75-86. Available from: https://doi.org/10.1108/13522750310470055 (Accessed 19 June 2005)

Rindfleisch, TC. 1997. *Privacy, information technology, and healthcare* 7-9.

Rodwin, MA. 2009. The case for public ownership of patient data. *JAMA*, 302(1):86–88

R.O.C.2009. Ministry of Health and Welfare. Regulations governing the utilization and management of electronic medical records among medical facilities. Available from: http://law.moj.gov.tw/ LawClass/LawAll.aspx?PCode=L0020121 (Accessed 12 May 2017).

Roney, K. 2012. Handle hospital data breaches with care: 5 issues to consider. *Becker's Hospital Review*, 14 November 2012. Available from: https://www.beckershospitalreview.com/healthcare-information-technology/handle-hospital-data-breaches-with-care-5-issues-to-consider.html (Accessed 28 June 2014).

Rosenzeig, P. 2009. *National security threats in cyberspace*. A workshop jointly conducted by American Bar Association Standing Committee on Law and National Security and National Strategy Forum.

Rosenbaum S., Abramson S & MacTaggart P. 2009. Health information law in the context of minors. *Pediatrics* 123: 116-121.

Rothstein, MA & Talbott, MK. 2007. Compelled authorisations for disclosure of health records: magnitude and implications. *American Journal of Bioethics* 7(3): 38-45.

Rozenblum, R., Jang, Y., Zimlichman, E., Salzberg, C., Tamblyn, M., Buckeridge, D., Forster, A., Bates, DW &Tamblyn, R. 2011. A qualitative study of Canada's experience with the

implementation of electronic health information technology. *Canadian Medical a Association Journal*, *183*(5):281-288.

RSA Anti-Fraud Command Center. 2010. RSA Online Fraud Report May 2010 [Online]. Available from: http://www.rsa.com/phishing_reports.aspx (Accessed 5 July 2010).

Rubin, A & Babbie, E. 2011. *Research methods for social work*. New York: Brooks/Cole Cengage Learning.

Ruf, L, Thorn, CA & Christen T. 2014. Threat modelling in security architecture – the nature of threats. ISSS Working Group on Security Architectures. Available from: http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture_Threat-Modeling_Lukas-Ruf.pdf (Accessed 18 May 1015).

Ruxwana, NL. 2010. *The adoption of quality assurance in e-Health acquisition for rural hospitals in the Eastern Cape Province.* Doctoral thesis, Nelson Mandela Metropolitan University, South Africa.

SA Justice Dept. 2009. Protection of Personal Information Bill of South Africa. Available from: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf (Accessed 26 November 2015).

Safran, C, Bloomrosen, M, Hammond, WE, Labkoff, S, Markel-Fox, S, Tang, PC & Detmer, DE. 2007. Towards a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association* 14(1): 1-9.

Salkind, Neil J & Kristin Rasmussen. 2007. *Encyclopedia of Measurement and Statistics*. (1st ed). Thousand Oaks, California: SAGE Publications.

Samadbeik, M, Gorzin, Z, Khoshkam, M & Roudbari, M. 2014. Managing the security of nursing data in the electronic health record. *Acta Informatica Medical* 23(1):39-43.

Samy, GN., Ahmad, R & Ismail, Z. 2010. Security threats categories in healthcare information systems", *Health Informatics Journal* 16 (3):201-209.

Samy, GN, Ahmad, R & Z. Ismail, Z. 2011. Health information security guidelines for healthcare information systems. *In ISHIMR 2011: proceedings of the 15th International Symposium for Health Information Management Research*, 8-9 September 2011, Zurich, Switzerland.

Sankar, P, Moran, S, Merz, JF & Jones, NL. 2003. Patient perspectives on medical confidentiality. *Journal of General Internal Medicine* 18(8): 659.

Saunders, M, Lewis, P & Thornhill, A. 2012. *Research methods for business students*. 6th ed. Harlow: Pearson.

Schattner, P. 2005. The GPCG computer security self-assessment guideline and checklist for General Practitioners. *East Bentleigh, Victoria, Australia: Department of General Practice, Monash University*.

Scot, MM. 2011. A primer on healthcare IT Myths, Realities, Risks and practical implications for trial lawyers. *Department of the Electronic Health Records, Virtual Mentor* 13(3): 86-189

Scotland, J. 2012. Exploring the philosophical underpinnings of research: relating ontology and epistemology to the methodology and methods of the scientific, interpretive and critical paradigms. *English Language Teaching* 5(9): 9-16.

Scott, R & Mars, M. 2015. Telehealth in the developing world: current status and future prospects. *Smart Homecare Technology and Telehealth*, 3: 25-37. Available from: https://www.dovepress.com/telehealth-in-the-developing-world-current-status-and-future-prospects-peer-reviewed-fulltext-article-SHTT (Accessed 17 July 2018).

Scott, M &Wingfield, N. 2017. Hacking attack has security experts scrambling to contain fallout, New York Times. Available from: https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-onlinesecurity-.security.html (Accessed 9 May 2017)

Scully, T. 2011. The cyber threat, trophy information and the fortress mentality. *Journal of Business Continuity & Emergency Planning* 5(3): 195-207.

Seahloli, MS. 2016. Current status of medical informatics and implementing electronic healthcare records, challenges, and future direction in South Africa. D.Phil. Thesis, Texila American University.

Serge, V. 2006. *A classical introduction to cryptography: applications for communications security*. Springer.

Shank, N, Willborn, E, PytlikZillig, L & Noel, H., Electronic health records: eliciting behavioural health providers' beliefs. *Community Mental Health Journal* 48(2): 249-254.

Shensul, JJ. 2012. Methodology, methods and tools in qualitative research. In S.D. Lapan, M.T. Quartaroli & F.J. Riemer (Eds.) *Qualitative research: introduction to methods and designs* (69-103). San Francisco: Jossey-Bass.

Shuttleworth, M. 2009. Writing a conclusion. Available from: https://explorable.com/writing-a-conclusion (Accessed 14 September 2015).

Singh, B & Muthuswamy, P. 2013. Factors affecting the adoption of electronic health records by nurses. *World Applied Sciences Journal* 28(11):1531-1535.

Sittig, DF. & Singh, H. 2011. Defining health information technology-related errors: new developments since *To Err Is Human*. *Archives of internal medicine* 171(14):1281-1284.

Sittig, DF & Singh, H. 2016. A socio-technical approach to preventing, mitigating and recovering from ransomware attacks. Applied Clinical Informatics 7(2): 627-628.

Siwicki, B. 2016. "Tips for Protecting Hospitals from Ransomware as Cyberattacks Surge," downloaded 8/27/16. Available from http://www.healthcareitnews.com/news/tips-protecting-hospitals-ransomware-cyber-attacks-surge (Accessed August 2016).

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.

Snell, E. 2015. Hacking still leading cause of 2015. Health IT Security. Available from: https://www.healthitsecurity.com/news/hacking-still-leading-cause-of-2015-health-databreaches(Accessed 19 February 2018).

Solander AC, Forman, AS & Glasser NM. 2016. Ransomware – Give me back my files! *Employee Relations Law Journal* 42(2): 53-55.

Solutions, VE. 2014. Verizon 2014 data breach investigations report. *Verizon. com* 13-15.

Song, S. 2017. *African undersea cables – Interactive*. Available from: https://manypossibilities.net/african-undersea-cables-interactive (Accessed 17 July 2018).

Spence, N, Paul III, DP & Coustasse, A. 2017. Ransomware in healthcare facilities: the future is now. Paper presented at the Academy of Business Research, Fall 2017 Conference, Atlantic City, NJ.

Srivastava, A & Thomson, S. 2009. *Framework analysis: a qualitative methodology for applied policy research*. Joaag.

Stone, A. 2010. A healthcare sector breach out of South Africa [Online]. Available from: http://www.phiprivacy.net/?p=2614 (Accessed 5 July 2010).

Stoneburner, G., Goguen, A & Feringa, A. 2002. Risk management guide for information technology systems. *NIST special publication* 800(30): 800-30

Strydom, H. 2005. Ethical aspects of research in the social sciences and human service professions. In AS. de Vos, H. Strydom, C.B. Fouche., & C.S.L. Delport (Eds), *Research at grass roots for the social sciences and human service professions* (56-85). Pretoria: Van Schaik Publishers

Terry, N. 2013. Protecting patient privacy in the age of big data. *UMKC Law Review,* 81(2). Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153269 (Accessed 17 July 2018).

Teddlie, C & Tashakkori, A. 2009. *Foundations of mixed methods research: integrating qualitative and quantitative approaches in the social and behaviour sciences*. London: Sage Publications.

Thomas, G. 2010. Doing case study: abduction not induction, phronesis not theory. *Qualitative Inquiry*, 16(7): 575-582. Retrieved from: http://dx.doi.org/10.1177/1077800410372601 (Accessed February 2010).

Thomson, LL. 2013. Healthcare data breaches and information security. In *American Bar Association* 253-267.

Tofan, DC. 2011. Information security standards. *Journal of Mobile, Embedded and Distributed Systems* 3(3): 128-135.

Trochim, WM, Donnelly, JP & Arora, K. 2016. *Research methods: the essential knowledge base*. New Delhi: Cengage Learning.

Tuyikeze, T & Pottas, D. 2005. Information security management and regulatory compliance in the South African health sector. In *ISSA 2005 New Knowledge Today Conference* (1-12).

Twigg, J. 2007. Tools for Mainstreaming Disaster Risk Reduction, Social Impact Assessment. International Federation of Red Cross and Red Crescent Societies ProVention Consortium. http://www.proventionconsortium.org /mainstreaming _tools (Accessed 12 June 2011).

Tyali, S & Pottas, D. 2011. Information security management systems in the healthcare context. *In Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010.*

United States Computer Emergency Readiness Team (US-CERT). 2016. Understanding Denial of Service (DoS) attacks. Available from: https://www.us-cert.gov/ncas/tips/ST04-015 (Accessed 4 July 2017).

US Department of Health and Human Services (HHS). 2014. Health information Privacy. Available from: http://www.hhs.gov/ocr/privacy. (Accessed 28 August 2014).

US Department of Health and Human Services (HHS). 2015. Fact sheet: ransomware and HIPAA [Internet]. Baltimore, MD: CMS. Available from: URL:http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. (Accessed: 08 September 2016).

US Department of Health & Human Services (HHS). 2016. The HIPAA Privacy Rule [Internet]. Washington (DC): US Department of Health & Human Services; c2016 [cited at 2017 Jul 1]. Available from: http://www.hhs.gov/ocr/ privacy/hipaa/administrative/privacyrule/. (Accessed 28 June 2018).

Vaast, E. 2007. Danger is in the eye of the beholders: social representations of information systems security in healthcare. *Journal of Strategic Information System* 16(2): 130-152.

Verizon. 2016. *Data breach Investigations Report*. Verizon.

Viswanath, K & Kreuter, MW. 2007. Health disparities, communication inequality and e-health: a commentary. *American Journal of Preventive Medicine* 32(5):131-133.

Vucetic, M, Uzelac, A & Gligoric, N. 2011. E-health transformation model in Serbia: design, architecture and developing. In *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2011), Beijing, China,* 566-573

Walker, JL. 2012. The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2): 37–46. Retrieved from www.ncbi.nlm.nih.gov/ (Accessed 7 July 2012).

Walsh, D., Passerini, K., Varshney, U & Fjermestad, J. 2009. Legal issues in the transition to electronic records in healthcare. *In Information Systems: People, Organisations, Institutions, and Technologies,* 321-326

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.

Wayne, D. 2012. *The research design maze: Understanding paradigms, cases, methods and methodologies*. Institute of Certified Management Accountants

Weaver, K & Olson, JK. 2006. Understanding paradigms used for nursing research. *Journal of Advanced Nursing* 53(4): 459-669.

Welman, C, Kruger, F & Mitchell, B. 2010. *Research methodology.* Oxford University Press: London.

Williams, PAH. 2005. The underestimation of threats to patient data in clinical practice. In *AISM* 117-122.

Williams, PAH & Mahncke, RJ. 2005. A new breed of risk: electronic medical records security. Paper presented at the 6th Australian Information Warfare and Security Conference, 24-25 November 2005, Melbourne, Australia.

Williams, PA & Woodward, AJ. 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, NZ)* 8: 305.

Winton, R. 2016. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating, Los Angeles Times, (2016). Available from: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html(Accessed19 February 2018).

World Health Organisation. 2012. Management of patient information: trends and challenges in member states: based on the findings of the second global survey on eHealth (Global Observatory for eHealth Series, v.6). Geneva: World Health Organisation.

World Health Organisation. 2018. *Health and sustainable development: energy access and resilience*. World Health Organisation.

Wright, G, O'Mahony & Cilliers, L. 2017. Electronic health information systems for public healthcare in South Africa: a review of current operational systems. *Journal of Health Informatics in Africa* 4(1):56-62.

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): 1820.

Zahoor, Z, Ud-din, M & Sunami, K. 2016. Challenges in privacy and security in banking sector and related countermeasures. *International Journal of Computer Applications* 144(3): 27.

Zarei J & Sadoughi F. 2016. Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Management Healthcare Policy*, 9:75-85. [http://dx.doi.org/10.2147/RMHP.S99908] [PMID: 27313481]

Yang, H & Bao, D. 2004. A smart-card-enabled privacy preserving E-prescriptions system. *Transaction on information technology in biomedicine* 8(1): 38.

Yarmohammadian, H, Raeisi, AR, Tavakoli, N & Nansa, LG. 2010. Medical record information disclosure laws and policies among selected countries; a comparative study. *Journal of Research in Medical sciences: the official journal of Isfahan University of Medical Sciences* 15(3):140.

Yau, HK. 2014. Information security controls. *Advanced in Robotics and Automation* 3(2): 1-3.

Yin, RK. 2013. Validity and generalization in future case study evaluations. *Evaluation*, 19: 321-332. Doi: 10.1177/1356389013497081

Yin, RK. 2014. *Research design and methods*. Los Angeles, CA: Sage Publications.

Yu, S, Wang, C, Ren, K & Lou, W. 2010, March. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (1-9). IEEE.

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 A: DATA PROTECTION LAWS AND REGULATIONS

Data protection laws and regulations in some of the countries

(Abouelmehdi et al 2017:73-80)

Country	Laws and Regulations	Features
U.S.A	*HIPAA Act Patient Safety and Quality Improvement Act (PSQIA)*	Requires the establishment of national standards for electronic healthcare transactions. Gives the right to privacy to individuals from age 12 through 18. Signed disclosure from the affected before giving out any information on provided healthcare to anyone, including parents. Patient Safety Work Product must not be disclosed (Data Protection Laws of the World 2017). Individual violating the confidentiality provisions is subject to a civil penalty. Protect security and privacy of electronic health information.
EU	*Data Protection Directive*	Protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data.
Canada	*Personal Information Protection and Electronic Documents Act ('PIPEDA')*	Individual is given the right to know the reasons for collection or use of personal information, so that organisations are required to protect this information in a reasonable and secure way.
UK	*Data Protection Act (DPA)*	Provides a way for individuals to control information about themselves. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.
Morocco	*The 09-08 act, dated on 18 February 2009*	Protects the one's privacy through the establishment of the CNDP authority by limiting the use of personal and

		sensitive data using the data controllers in any data processing operation.
Russia	*Russian Federal Law on Personal Data*	Requires data operators to take "all the necessary organisational and technical measures required for protecting personal data against unlawful or accidental access".
India	*IT Act and IT (Amendment) Act*	Implement reasonable security practices for sensitive personal data or information. Provides for compensation to person affected by wrongful loss or wrongful gain. Provides for imprisonment and/or fine for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.
Brazil	*Constitution*	The intimacy, private life, honour and image of the people are inviolable, with assured right to indenization by material or moral damage resulting from its violation.
Australia	*New South Wales Health Records and Information Privacy Act (NSW HRIPA)*	Health records can only be used for the purposes stated to the patient; any secondary use must be requested unless it is an emergency. Disclosure of data is prohibited outside of consented purpose and authorised individual.
Angola	*Data Protection Law (Law no. 22/11of 17 June)*	With respect to sensitive data processing, collection and processing is only allowed where there is a legal provision allowing such processing and prior authorisation from the APD is obtained.
Taiwan	*Computer Processed Personal Information Protection Act*	To protect personal information processed by computers. Prohibits individuals from waiving certain rights.
New Zealand	*Privacy Act*	Sets out principles in relation to the collection, use, disclosure, security and access to personal information
Singapore	*National Medical Ethics Committee Act*	

Malaysia	*Private Healthcare Facilities and Services Act*	
South Africa	*Protection of Personal Information Act (POPI)*	POPI act provide a set of principles to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way.
	Promotion of Access to Information Act (PAIA)	PAIA promote and enforce open access to information in possession of government entities or institutions. The main aim is to ensure the protection of people's rights
	National Health Act, No 61 of 2003 (Health Act)	National Health Act protects the privacy and confidentiality of patient records (which includes information pertaining to a patient's health status, treatment or stay in a health establishment) and provides, in particular, that such information may only be disclosed if the patient consents to disclosure in writing, or a court order or law justifies such disclosure.
Sweden	*The Personal Data Act (SFS 1998:204)*	Provisions to protect the personal integrity of people (patients in healthcare). The Act, which is adapted to EU rules, applies to personal data that is transmitted, disseminated or made available by other means.

APPENDIX B: ISO STANDARDS

ISO 27001	This is the specification for an information security management system (an ISMS) and replaces the old BS7799-2.
ISO27002	This is the potential new standard number of the existing ISO 17799 standard (which itself was formerly known as BS7799-1) and outlines a code of practice for information security.
ISO27003	This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (IS Management System).
ISO 27004	This is the designated number for a new standard covering information security system management measurement and metrics
ISO27005	This is the ISO number assigned for an emerging standard for information security risk management.
ISO27006	This standard will provide guidelines for the accreditation of organisations offering ISMS certification.

APPENDIX C: INTERVIEW GUIDE

UNISA university of south africa

INTERVIEW GUIDE

Student: Kabelo Given Chuma

Student number: 50119869

Title: SECURITY OF ELECTRONIC PERSONAL HEALTH INFORMATION IN A PUBLIC HOSPITAL IN SOUTH AFRICA

I would like to do an interview with you concerning the security of ePHI in your hospital. I would like you to answer according to your point of view and express your opinions. All the answers you give me will be confidential and only be used for the purpose of this study. I will only take your name for my record only.

The initial interview schedule will cover the following broad areas:

- ✓ Demographic information
- ✓ Legislative framework and policies
- ✓ Security threats
- ✓ Security control measures
- ✓ Privacy issues
- ✓ Recommendations

Section A: Demographic information

1. What is your job title or position in the hospital?

_____

_____

_____

_____

2. What does your job entails?

_____

_____

_____

_____

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

3. How long have been working in the hospital?

4. What other branches do your hospital have?

5. What is your highest academic qualification?

Section B: Legislative framework and policies

6. Which legislative framework does your hospital use to guide the security of ePHI?

7. How do you apply the legislative framework in governing the security of ePHI?

8. Which international security standards does your hospital use to cover the security of ePHI?

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

9. What policies and procedures does your hospital have to protect ePHI?

10. How does your hospital implement and enforce these policies and procedures?

Section D: Security threats

11. What security threats to ePHI have you ever experienced in your hospital?

12. How do you prevent and respond to security threats to ePHI?

Section C: Security control measures

13. What system are you using for ePHI?

14. What standards is the hospital system certified against?

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

15. What other systems are integrated with the ePHI system?

16. What security control measures are in place to protect ePHI in the hospital?

17. Explain how effective and reliable these security control measures are?

18. Who have access to ePHI in your hospital?

19. How access to ePHI is controlled in your hospital?

20. What kind of access controls does your hospital use to prevent unauthorised access to ePHI?

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Section E: Privacy issues

21. What privacy issues have been raised against the hospital?

22. How do you handle privacy issues that arises?

Section F: Recommendations and suggestions

23. What future plans does the hospital have with respect to the security of ePHI?

24. In your opinion, what should be done to improve the security of ePHI in general in your hospital?

We have come to the end of this interview, thank you for participating in this study!!!

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

We have come to the end of this interview, thank you for participating in this study!!!

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX D: UNISA ETHICAL CLEARANCE LETTER

UNISA university of south africa

DEPARTMENT OF INFORMATION SCIENCE ETHICS REVIEW COMMITTEE

20 March 2019

Dear Mr Kabelo Given Chuma

DIS Registration #: Rec-190319

References #: 2019-DIS-0007

Name: K G Chuma

Student #: 50119869

Decision:

Ethics Approval from 19 March 2019 to 19 march 2024

Researcher: Mr Kabelo Given Chuma
50119869@mylife.unisa.ac.za

Supervisor: Prof MS Ngoepe
ngoepms@unisa.ac.za

Security of electronic personal health information in a public hospital in South Africa.

Qualifications: Masters Dissertation

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Thank you for the application for research ethics clearance by the Unisa Department of Information Science Research Ethics Committee for the above-mentioned research. Ethics approval is granted for five years.

The ***low risk application*** was reviewed and expedited by the Department of Information Science Research Ethics Committee on 19 March 2019 in compliance with the Unisa Policy on Research Ethics and the Standards Operating Procedure on Research Ethics Risk Assessment. The proposed research may now commence with the provisions that:

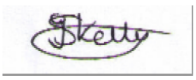
1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy of Research Ethics.
2. Any adverse circumstances arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the Department of Information Science Ethics Review Committee.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards the protection of participants' privacy and the confidentiality of the data should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no. 4 of 2013; Children's Act no. 38 of 2005 and the National Health Act, no. 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date of **19 March 2024**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

*The reference number **2019-DIS-0007** should be clearly indicated on all forms of communication with the intended research participants, as well as the Committee.*

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Yours sincerely



Dr Isabel Schellnack-Kelly
Department of Information Science: Ethics Committee

APPENDIX E: LETTER SEEKING PERMISSION TO CONDUCT RESEARCH IN A PUBLIC HOSPITAL

DEPARTMENT OF INFORMATION SCIENCE
P O BOX 392
UNISA
0003
TEL: 012 429 3902
chumakg@unisa.ac.za

UNISA university of south africa

TO: [redacted]
FROM: **Mr Kabelo Chuma**
DATE: **15 July 2019**

REQUEST FOR PERMISSION TO CONDUCT RESEARCH STUDY IN THE HOSPITAL

The above matter refers:

My name is Kabelo Given Chuma, and I am a Master's student at the University of South Africa in Pretoria. The research I wish to conduct for my Master's research entitled **"Security of Electronic Personal Health Information (ePHI) in a public hospital in South Africa".** I have chosen [redacted] to serve as a case study for my research study. This project will be conducted under supervision of Professor Mpho Ngoepe (University of South Africa).

I have made significant progress with my research study and I am now at the stage of data collection. I wish to request permission to interview members of the hospital who constitute my sample population. The study involves face-to-face semi-structured interviews. The interviews will be conducted with the selected IT staff, administrative staff, records management staff and system security staff working in the hospital. Appointments will be scheduled on a date of the participant's availability and will be secured by the researcher before the commencement of interviews to enable participants to prepare adequately for the interview. For the purpose of this study, the researcher will ask questions and probe according to the respond of the participants. Data will be collected using a tape recorder to capture responses and field notes will be taken to support the recorded information. The researcher will collect data on a daily for a period of four weeks until the desired results are reached.

Participation is voluntary and informed consent will be obtained from participants. A comprehensive written information form regarding the research will be provided to the participants. In this study, the researcher will not access any patient's health information in the hospital system but to gain in-depth understanding about the security of ePHI against various

threats and risks. For the purpose of this study, anonymity will be ensured. The name of the hospital will, of course, be treated anonymously and the names of the participants will be not provided. In addition to this, responses from participants and records will be kept strictly confidential.

It is my hope that the outcome of this research study will accrue dual benefits by satisfying the requirement for the award of a Master's degree, while providing useful insight and information that would improve the security of ePHI in your hospital in particular. Upon completion of this study, all the participants who played a role in this study will be informed of the outcome of the study.

Should there be any enquiries about this research study, please do not hesitate to contact my supervisor, Prof Mpho Ngoepe: 012 429 6360: e-mail: ngoepms@unisa.ac.za, at the Department of Information Science, School of Arts, College of Human Sciences, UNISA.

The research proposal and ethical clearance documents for the study were submitted to the Higher Degrees Committee of the University of South Africa for approval, the Committee approved the proposal, and an ethical clearance was granted.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Your approval to conduct this will be highly appreciated

Regards

Kabelo Given Chuma
Tel: 012 429 3902
Cell: 0787972343
Email: chumakg@unisa.ac.za

APPENDIX F: LETTER OF PERMISSION TO CONDUCT RESEARCH IN A PUBLIC HOSPITAL

GAUTENG PROVINCE
HEALTH
REPUBLIC OF SOUTH AFRICA

Enquiries: Mpho Moshime-Shabagu
Tel: +27 12 451 9036
E-mail: Mpho.Moshime@gauteng.gov.za

TSHWANE RESEARCH COMMITTEE: CLEARANCE CERTIFICATE

DATE ISSUED: 14/08/2019
PROJECT NUMBER: 48/2019
NHRD REFERENCE NUMBER: GP_201907_025

TOPIC: Security of Electronic Personal Health Information (ePHI) in a selected hospital in South Africa

Name of the Researcher:	Mr Kabelo Given Chuma
Name of the Supervisor:	Prof Ms Ngoepe
Facility:	[redacted]
Name of the Department:	UNISA

NB: THIS OFFICE REQUEST A FULL REPORT ON THE OUTCOME OF THE RESEARCH DONE AND

Text

NOTE THAT RESUBMISSION OF THE PROTOCOL BY RESEARCHER(S) IS REQUIRED IF THERE IS DEPARTURE FROM THE PROTOCOL PROCEDURES AS APPROVED BY THE COMMITTEE.

DECISION OF THE COMMITTEE: APPROVED

.....
Dr. Mpho Moshime-Shabangu
Acting Chairperson: Tshwane Research Committee

Date 14/08/2019

.....
Mr. Mothomone Pitsi
Chief Director: Tshwane District Health

Date: 2019.08.14

APPENDIX G: INFORMED CONSENT

INFORMED CONSENT FORM

Title of the study: Security of Electronic Personal Health Information in a public hospital in South Africa

Degree: Masters in Information Science

Institution: University of South Africa

Researcher: Kabelo Chuma (+27 78 797 2343; kabelo.chuma@gmail.com)

Supervisor: Prof Mpho Ngoepe (+27 83 418 4688; ngoepms@unisa.ac.za)

The study explores the security of electronic personal health information (ePHI) in a public hospital in South Africa. The ultimate goal of this study is to understand how patient's data is protected. I humbly request your time to participate in this interview that is guided by questions structured in such a way that your responses will yield data that will address some of my research questions. **The interview will take about 20-30 minutes**. Please note that all responses will be presented anonymously and treated confidentially. Your participation is voluntary and do not feel you are obliged to answer all questions particularly those that make you feel uncomfortable. You have the right to withdraw anytime and nothing will be held against you.

If you have any questions or contribution regarding this research, please feel free to ask me; you are also welcome to contact me or my supervisor.

Confirmation of informed consent to be interviewed:

(Please initial at the end of each line if you agree)

I understand the background of this study and have asked any clarifying questions I

wish _____

I understand I am participating voluntarily and may withdraw at any point_____

I understand that I am not obliged to answer all questions_____

I agree to this interview being recorded _____

I _____ agree to participate in the

Study described above.

Signature _____Date_____

APPENDIX H: DECLINED APPLICATION LETTER

[redacted]

[redacted]
Oxford Manor, 21 Chaplin Road, Illovo 2196
Private Bag X13, Northlands 2116, South Africa
Telephone: +27 11 219 9000
Telefax: +27 11 219 9001
[redacted]

National Health Research Ethics Committee registration: REC 251015-048

Ref: 07042019/1

04 July 2019

ATTENTION: Kabelo Chuma

APPLICATION TO CONDUCT RESEARCH STUDY: DECLINED

TITLE: Security of Electronic Personal Health Information (ePHI) in a private hospital in South Africa

The Research and Ethics Committee of Life Healthcare has not granted permission for your study to be conducted at Life Healthcare facilities due to the following reasons:

1. Disclosure of the information requested poses a security risk to Life Healthcare Group.

We wish you well with your study.

Yours sincerely,

[redacted]
On behalf of the Research & Ethics Committee

APPENDIX I: DECLINED APPLICATION LETTER

[redacted]

[redacted]
Tel: + 27 (0)11 301 0000
Fax: Corporate +27 (0)11 301 0499
76 Maude Street, Corner West Street, Sandton, South Africa
Private Bag X34, Benmore, 2010, South Africa

RESEARCH OPERATIONS COMMITTEE- DECLINE OF APPLICATION

Approval number: UNIV-2019-0038

Kabelo Given Chuma
Email: chumakg@unisa.ac.za
Phone: 078 79 72 343

Dear Mr Chuma

RE: SECURITY OF ELECTRONIC PERSONAL HEALTH INFORMATION (ePHI) IN A PRIVATE HOSPITAL IN SOUTH AFRICA

The above-mentioned research was reviewed by the Research Operations Committee's delegated members and has unfortunately been declined for the following reasons:
Netcare is not in a position to support the request for the specific data as it is deemed to be confidential.

Yours faithfully

[redacted]
Prof Dian du sis
Full member: etcare Research Operations Committee & Medical Practitioner evaluating research applications as per Management and Governance Policy

[redacted]
Shannon Nell
Chairperson: Netcare Research Operations Committee
Netcare Hospitals (Pty) Ltd
Date: Nov dB/ '1