University of Fort Hare

Together in Excellence

A Privacy Management Framework for Mobile Personal Electronic Health Records in South Africa

By

Floyd Nathaniel Els

A Privacy Management Framework for Mobile Personal Electronic Health Records in South Africa

by

Floyd Nathaniel Els
200901461

Dissertation

Submitted in fulfilment of the requirements for the degree

Masters of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: **Dr Liezel Cilliers**

May 2017

Abstract

South Africa's health status is in constant dismay, especially while under the strain of the quadruple burden of disease. The adoption of personal electronic health records (PEHRs) can be seen as a means to improve this status by empowering patients to manage their health and lifestyle better. While from the healthcare provider's perspective, PEHRs has the ability to reduce medical errors; provide better communication channels and enhance the monitoring of patients. Despite these benefits for both healthcare providers and patients, there are three distinct information security threats relating to PEHRs. These threats refer to the individual, data in transit, and at rest.

South Africa is still considered to be inexperienced with PEHRs, and consider it a relatively new concept to the healthcare system. The National e-Health Strategy and Protection of Personal Information Bill were discussed and compared to international standards in order to ascertain South Africa's current standing on mobile healthcare privacy. However, there are no specific privacy and security controls in place to protect patients that access personal electronic health records through mobile devices. Therefore, the aim of this study is the development of a privacy management framework (PMF) to mitigate these privacy concerns. Following an interpretivistic approach to research, qualitative data was analysed from literature, and the privacy framework evaluated through expert reviews.

The proposed PMF consists of 3 tiers, beginning with the top tier. The first tier relates to an organisations interpretation and understanding of data privacy laws and regulations, and in ensuring compliance with these laws. The second tier refers to two support pillars to maintain the first tier. These pillars are based on elements of operational privacy, as well as auditing and reviewing. The third tier serves as the basic foundation upon which the PMF was developed. It is mainly focused with creating privacy awareness amongst healthcare providers and patients by creating: training regimes on security and privacy threats, efficient communication standards, and constant ongoing support from top level management.

Declaration

I, **Floyd Nathaniel Els**, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised institution.
- I am fully aware of the University of Fort Hare's policy on research ethics and I have taken every precaution to comply with the regulations.

Signature: _____

Date: 15 May 2017

Acknowledgements

I would like to thank my supervisor, my lecturer, my friend, and my mentor Dr. Liezel Cilliers. Without your guidance, your encouragement and wilfulness over these months, I would never have dreamed of getting this far. Thank you for always pushing and directing not only me, but all of us. Your experience and commitment will always be greatly appreciated and never forgotten.

I would also like to thank my colleagues and the experts who have constantly provided input in achieving this milestone.

A special acknowledgement to the Swedish Research Council for Health, Working Life and Welfare (Forte) and the Council for Scientific and Industrial Research (CSIR), thank you both for the opportunity at a scholarship, I would have not been able to complete this research study without it.

My parents, family and friends, thank you the continuous support and love. I would not be where I am today without you all.

To Alisha, words will never be enough, but always remember, “More than yesterday, but never more than tomorrow”.

Table of Contents

List of Appendices

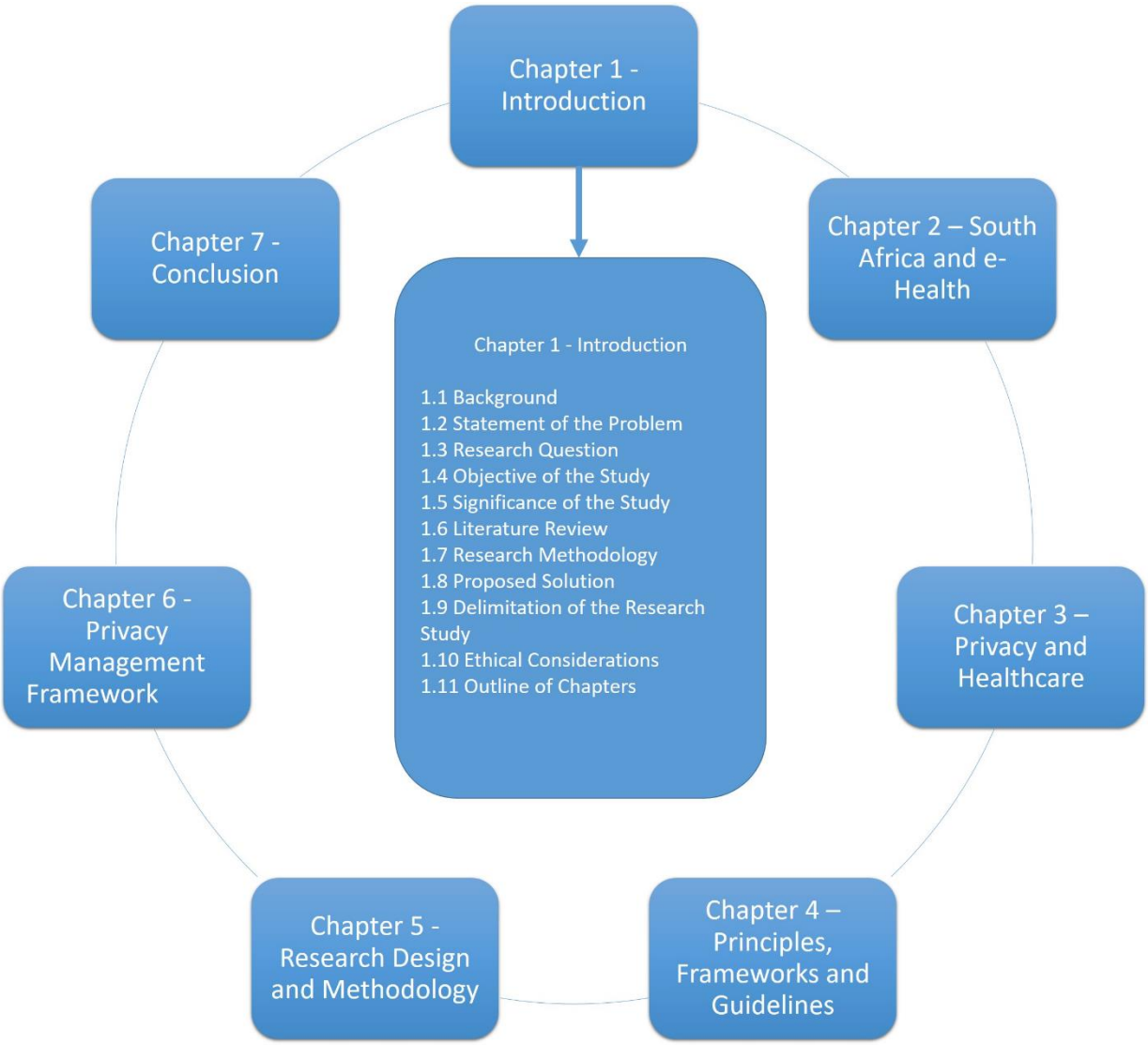
List of Acronyms

AIDS	Acquired Immune Deficiency Syndrome
APP	Australian Privacy Principles
CF	Markle Common Framework
CIA	Confidentiality, Integrity and Availability
e-Health	Electronic Health
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
HIV	Human Immunodeficiency Virus
ICT	Information and Communications Technology
IS	Information Systems
IVF	In Vitro Fertilization
m-Health	Mobile Health
NHI	National Health Insurance Act
OAIC	Office of the Australian Information Commissioner
OECD	Organization for Economic Cooperation and Development
ONC	Office of the National Coordinator for Health Information
PCPD	Hong Kong's Office of the Privacy Commissioner for Personal Data
PEHR	Personal Electronic Health Records
PII	Personally Identifiable Information
PMF	Privacy Management Framework
PMP	Privacy Management Programme
PoPI	Protection of Personal Information Act
SSRC	Social Science Research Centre of the University of Hong Kong
TB	Tuberculosis
UNC	University of North Carolina
USAID	United States Agency for International Development
USB	Universal Serial Bus

List of Figures

List of Tables

Chapter 1: Introduction



1.1 Background

The collection of patient information is a common practice across all healthcare organisations, including medical centres, general practitioners and even insurance companies. In order to ensure that a patient's information is up to date, many healthcare organisations are making use of electronic record keeping systems (Healthcare Information and Management Systems Society, 2014).

One type of an electronic record is called a personal electronic health record (PEHR). A PEHR is described as a health record where a patient's health data and information is managed and controlled by the patient. This information may include, but is not limited to, family and chronic history, surgeries and procedures as well as prescription records (Tang, Ash, Bates, Overhage & Sands, 2006). Collecting health information in one repository creates an effective communication pathway between patients and healthcare providers as relevant information can be shared. Furthermore, PEHRs can assist in reducing medical errors and enhance the monitoring of health conditions. This enables the patients to improve their health status as they are equipped to monitor their health information more effectively (Bouri & Ravi, 2014). However, the information pertained in a PEHR does not replace the legal records of a healthcare provider (Givens & Cordary, 2012).

A patient's health information is considered to be sensitive and private. Privacy refers to the ability of an individual to isolate information about oneself, while being able to express this information selectively (Oulasvirta, Suomalainen, Hamari, Lampinen & Karvonen, 2014). Therefore, if PEHRs are to assume a fully integrated and successful role in the delivery of healthcare, there must be controls in place that will ensure the patient's privacy (Oulasvirta et al., 2014).

An individual is able to manage and control their PEHR through the use of commercially available applications that range from mobile devices to Web-based or Cloud-based services, creating more accessibility and convenience for patients (Tang et al., 2006; Bouri & Ravi, 2014). However, PEHRs is still considered a relatively new concept in the healthcare sector of South Africa (Erasmus, 2014; Mxoli, Mostert-Phipps, & Gerber, 2014). Furthermore, as most PEHRs services are being outsourced by the healthcare organisation to a third party, there are security and privacy concerns about storage and distribution of patient information (Mahajan & Patel, 2012).

According to recent research studies done by the Pew Research Centre (2015), South Africa and Nigeria were identified as two of the countries with the highest mobile device ownership in Africa,

with 90% of people in these countries owning a mobile device. The prevalence of mobile devices means that it is likely that in the future, patients will access their PEHRs making use of these devices. However, there are several problems that can affect an individual's right to privacy when making use of mobile devices to manage their healthcare. As mobile devices are portable in nature, they are commonly prone to theft, loss or damage (Srivastava, Hossain, & Koekemoer, 2012). The second issue refers to messages in transit, as they may be susceptible to eavesdropping and recording (Srivastava et al., 2012). Taitsman, Grimm, and Agrawal (2013) argue that "The risk of electronic eavesdropping further complicates healthcare providers' responsibility to protect patient privacy" (p. 978). As such, regulations and policies need to be implemented to safeguard the data residing on these mobile devices and to further govern these privacy concerns (Srivastava et al., 2012).

The legislative environmental structure in South Africa is considered to be continuously developing and changing (Kingwill, 2016). As a result, South Africa has introduced the Protection of Personal Information Act (PoPI) of 2013. This act attempts to address the security and privacy concerns in the collection of personal information, however, it is not entirely sufficient for a digital environment (Townsend & Ncube, 2013; Botha & Booi, 2016).

The conceptual privacy mobile (m)-Health framework provides an international perspective of privacy that can be implemented in an m-Health environment (Avancha, Baxi, & Kotz, 2012). The adaption of this framework for the South African context would contribute to the mitigation of privacy concerns. Therefore, healthcare providers would be able to use the PoPI Act and the framework as guidelines to increase the privacy management of PEHRs. The following section explains the problem statement and the research question.

1.2 Statement of the Problem

In a research initiative conducted by the United States Agency for International Development (USAid) and the University of North Carolina (UNC), known as 'Measure Evaluation', the importance of m-Health for healthcare delivery in South Africa is identified. Through this research, the innovations in m-Health technologies have shown effective methods to improve access to health services and information. However, the study also found that there are constraints with m-Health programmes in South Africa, which include developing privacy and security standards for mobile technologies (USAid, 2016). Plachkinova, Alluhaidan and Chatterjee (2015) state that "The patient should be the one to have control of how data is used and accessed" (p. 4). Furthermore, the service must be delivered in an environment in which patients have absolute

confidence that their privacy will be protected. Additionally the confidentiality, integrity and availability of the information stored in PEHRs must be assured (Fineberg & Brandt, 2014). While it is important to distinguish between the concepts of privacy and information security as applied to healthcare data, it is particularly important to do so for PEHRs. Thomson (2013) argues from an organisations' perspective that there is a high cost associated with a breach of personal information, such as the potential liability, negative publicity and loss of the patients' trust in the healthcare provider (Privacy Commissioner for Personal Data, 2014). These threats would probably "affect a patient's safety and privacy and confidentiality and integrity of healthcare data" (Hsu et al., 2015, p. 1).

The PoPI Act introduced by South Africa sets to govern these privacy concerns, but is not specifically designed for the mobile health environment (Calaguas, 2013). The MEASURE Evaluation research project had examined the current legal framework of South Africa, and in particular, noted the importance of the PoPI Act for any m-Health initiative. However, as stated in the research, "The act aims to give minimum requirements for the processing of personal information" (USAid, 2016, p. 1). The problem therefore, is that healthcare providers must be able to protect the privacy of PEHRs that are accessed on mobile devices for their patients. The following section will discuss the research question and its sub-questions.

.

1.3 Research Question

This section provides the main question of this research study. It will also outline and explain the three sub-questions formulated to aid in answering the main research question:

How can healthcare providers mitigate privacy concerns of South African patients making use of mobile devices to access personal electronic health records?

1.3.1 Sub Questions

The main research question above has been answered through the following sub-questions:

1) How can mobile personal health records improve patient management?

This question focused on how effective mobile health records are for managing patient information from both the healthcare-provider and patient's perspective.

2) What are the privacy concerns of a South African patient making use of mobile devices to manage their data?

This second sub-question discussed the various types of privacy concerns patients experience whilst using a mobile device to manage their personal information.

3) How can a privacy management framework ensure the privacy of South African patients?

This last sub-question identified and discussed how a privacy management framework would be able to assist in ensuring privacy amongst patients that use personal electronic health records. This section provides the main research question for this study which is then broken into sub-questions in order to provide a solution to the main research question. The following section discusses the main objective of this study.

1.4 Objective of the Study

The primary objective of this study was to develop a privacy management framework through which the effectiveness of PEHRs for managing health data could be examined. Furthermore, healthcare providers would be able to mitigate privacy concerns of patients making use of mobile devices to manage their PEHRs. Although PoPI was introduced in South Africa to legislate the use of private information, it does not specifically make provision for electronic data gathering or health care information (Calaguas, 2013). This study will propose a privacy management framework that, in conjunction with the conceptual privacy m-Health framework, attempts to solve both these issues.

1.5 Significance of the Study

The importance of this study is to ensure that South African patients, whom have access to PEHRs on their mobile devices, are assured of the privacy of their healthcare information. In addition, if PEHRs are used more often in South Africa, the standard and continuity of patient care would improve (Kharrazi et al., 2012).

1.6 Literature Review

In this section a theoretical foundation is provided and relevant theory discussed. The first section discusses the effectiveness of health records for managing patient information. This is followed by privacy concerns which patients experience while using a mobile device to access their PEHRs. The last section compares various frameworks and theories that may be implemented to govern the privacy of PEHRs on mobile devices.

1.6.1 The Effectiveness of Personal Electronic Health Records

PEHRs have the potential to share information between a patient and a healthcare provider. This information can pertain to the diagnosis of medical conditions, clinical summaries, prescribing prescriptions, appointment reminders and even educational resources, regardless of any geographical and time constraint (Bouri & Ravi, 2014). The continuity and quality of medical care can be increased if both patients and healthcare providers have access to their PEHRs. Patients that visit many clinics or doctors are able to take the responsibility for the currency of their records as they are maintaining them, and furthermore sharing the records with authorised healthcare providers (Bouri & Ravi, 2014).

It has been noted that patients are increasingly searching for more accessible and portable methods for maintaining their PEHRs. The reason why PEHRs should be accessible is to be able to provide critical medical information in times of emergencies (Kharrazi et al., 2012). Initially, personal devices such as CDs and electronic storage drives were used to store this critical medical information. However, these devices were affected by significant limitations, such as requiring computer and supplementary software to access the devices. Additionally, the devices could be damaged and the data corrupted or lost (Steele, Min, & Lo, 2012).

In order to address these concerns, Kharrazi et al. (2012) state that cellular phones and tablet computers could be used as a new platform for PEHRs. Furthermore, individuals are becoming more technologically savvy with the increased use of and access to mobile devices. In a recent study by the Pew Research Centre (2015), it is identified that up to 89% of South African adults own a cell phone, highlighting the fact that mobile devices are a suitable alternative to access PEHRs. Mobile devices however, cannot preserve patient privacy, as security measures are still being developed for these devices (Fineberg & Brandt, 2014; Plachkinova et al., 2015). Restrictions such as restricted battery life, storage and processing power when compared to desktop computers limit the security features of mobile devices. The following section briefly discusses privacy threats experienced by patients that utilise mobile devices.

1.6.2 Threats to Privacy

In a research survey conducted by Avancha et al. (2012), and further discussed by Els and Cilliers (2017) (see Appendix A), the most common privacy threats relating to mobile devices and use of PEHRs were identified. The first threat relates to identity, whereby a patient misplaces their mobile device or inadvertently shares their identity credentials. This enables an unauthorised individual access to breach their privacy (Avancha et al., 2012). Furthermore, an individual might

use a patient's identity to obtain medical services, which could lead to financial consequences for the patient (Johnson, 2009; Taitsman et al., 2013).

The second threat identified relates to the access of PEHRs. Patients may mistakenly modify their own data incorrectly if the access-controls are too permissive. As such, a patient may intentionally modify their personal information to gain reimbursement through financial fraud or malice (Dixon, 2006; Taitsman et al., 2013). The last privacy threat identified relates to the disclosure of the information within PEHRs, which includes data at rest and in transit. This information may be disclosed inadvertently by a patient or an individual with access, allowing data disclosure beyond the intended purposes (Avancha et al., 2012). The disclosed information may be utilised for financial gain or to humiliate the patient (Appari & Johnson, 2010).

One such example where safeguards failed occurred in 2013. A medical technician at the Howard University Hospital in Washington used his/her position to gain access to confidential patient information, and attempted to sell the information over a 17-month period before being caught. Additionally, an external contractor for the same hospital had downloaded more than 34 000 patient files to their mobile device before it was stolen (Ozair, Jamshed, Sharma, & Aggarwal, 2015). The following section will discuss the conceptual m-Health privacy framework, followed by the South African Protection of Personal Act (PoPI) of 2013, while finally evaluating the impact of the privacy management framework.

1.6.3 Conceptual m-Health Privacy Framework

The conceptual m-Health privacy framework was developed upon the requirements of various international security policies and standards, but designed to be implemented for a mobile health platform (Avancha et al., 2012). This privacy framework consists of several principles that involve the responsibility of a healthcare provider to inform a patient of what information has been collected about him/her, as well as the purpose of this information (Markle Common Framework, 2008). Furthermore, the information collected is to be accurate, complete and timeously updated (HIPAA, 2010; Markle Common Framework, 2008; ONC National Framework, 2008). Additionally, administrative, technical and physical safeguards by healthcare providers must be in place to protect patient information both physically and electronically. However, remedies should be prepared to be implemented in the situation of a privacy breach (HIPAA, 2010; ONC National Framework, 2008). The following section discusses the Protection of Personal Information Act.

1.6.4 Protection of Personal Information Act

South Africa has introduced the Protection of Personal Information Act of 2013 (PoPI) to regulate the processing of personal information. Although this Act is not specifically designed to protect privacy in healthcare information, the PoPI Act prescribes that personally identifiable information (PII) contained in a patient's medical records must be protected (Calaguas, 2013). As such, the purpose of the Act is to provide a constitutional right to individual privacy and to safeguard any personal information when processed by a responsible party (SA Justice Department, 2013). Additionally, the responsible party must take reasonable and practicable steps in ensuring that if personal information is processed, it is to be for explicitly defined and legitimate reasons. Furthermore, any personal information collected is accurate, reliable and complete (Basson & Van Zyl, 2014). However, as stated by Tuyikezea and Pottas (2005), "being compliant with all legal requirements does not guarantee privacy and security protection of health information" (p.11). The following table compares how the PoPI Act correlates with the guidelines of the conceptual framework for m-Health privacy.

Table 1 - Comparison of the South African Protection of Personal Information Act and Conceptual Framework for m-Health Information Privacy Principles (adapted from Dala & Venter, 2015)

Conceptual Framework for m-Health Information Privacy Principles	PoPI Requirement Addressed
Openness and Transparency	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 6**)
Purpose Specification	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 3** and **4**)
Collection Limitation and Data Minimization	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 2, 3** and **4**)
Use Limitation (Transitive)	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 2, 3** and **4**) - and Chapter 6: Prior Authorisation
Individual Participation and Control	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 8**)
Data Quality and Integrity	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 5**)
Security Safeguards and Controls	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 7**)
Accountability and Remedies	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 1**) - deals with Accountability - while (**Condition 7**) - provides provision that a patient is to be alerted in the event of a data breach. Furthermore, Chapter 5: Supervision - introduces the information regulator which will be the privacy enforcement regulator.
	For the implementation of this principle, there is no specific reference to a privacy management framework. However, Chapter 11: Offences, Penalties and Administrative Fines - makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintaining good policies, procedures and practices to protect personal information.
Patient Access to Data	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 6** and **8**)
Anonymity of Presence	Not addressed in the PoPI Act

Table 1 provides the comparison of the common principles between PoPI Act and the conceptual m-Health framework, but there are exceptions present within the PoPI Act (Els & Cilliers, 2017). One instance relates to the absence of a privacy management framework which will be briefly discussed in the next section.

1.6.5 Privacy Management Framework

A privacy management framework (PMF) serves as a strategic framework which is able to assist an organisation in developing a robust privacy framework. This framework is able to identify any weaknesses within the organisation, as well as improve their good practises and potentially increase the protection of personal data. Alternatively, without an efficient data protection plan, personal data breaches can be detrimental and expensive to an organisation in terms of repairing reputations and trust (Australian Information Commissioner, 2015; Privacy Commissioner for Personal Data, 2014).

The Australian Government has developed their own privacy management framework through a four step guideline process. These steps refer to the embedment of a privacy culture to enable organisational compliance; establishing a robust and effective privacy process; evaluating these processes to ensure continuous effectiveness and lastly enhancing responses to privacy issues (Australian Information Commissioner, 2015). While the Hong Kong Government has similar in-depth privacy framework guidelines, its focus is on creating organisational commitment and implementing programme controls. This refers to the integration of a privacy culture throughout an organisation with top-management commitment; a continuous risk assessment analysis; policy training and education for those that interact with personal data; communicating privacy concerns and continuously assessing and reviewing the privacy framework (Privacy Commissioner for Personal Data, 2014). Additionally, the Organization for Economic Cooperation and Development from Sweden provided a forum on which governments can compare policy experiences and seek answers to common problems (Kuschewsky, 2014). The following section will discuss the research methodology.

1.7 Research Methodology

According to DePoy and Gitlin (2015), research is defined as "multiple, systematic strategies to generate knowledge about human behaviour, human experience and human environments in which the thinking and action processes of the researcher are clearly specified so that they are logical, understandable, confirmable, and useful" (p. 1). The following sections will review the research methodology, paradigm, approach and design. Thereafter, the study population and sampling

techniques will be investigated. This is followed by the data collection tools and analysis methods that will be utilised in this study.

1.7.1 Research Paradigm

Saunders, Lewis, and Thornhill (2009) consider a research paradigm as a means to study social phenomena from which certain understandings can be achieved.

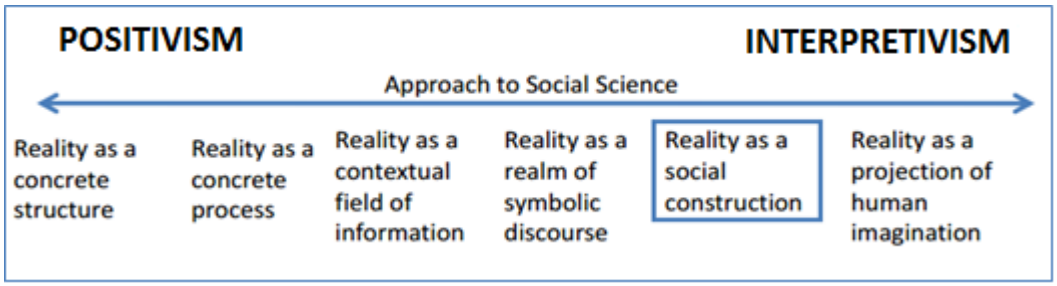


Figure 1 - Continuum of Core Ontological Assumptions (Collis & Hussey, 2013)

People are considered to be in a continuous process of interpreting the social world around them; as such they interpret the actions of others with whom they interact. This interpretation leads to the modification of a person's actions and understanding. Illustrated in Figure 1, the Continuum of Core Ontological Assumptions indicates that this study aligns with the fifth stage of the Continuum: "Reality as a Social Construction". Collis and Hussey (2013) state that "individuals through language, actions and routines create the social world" (p. 49). Therefore, for this research study an interpretivist approach was considered appropriate as qualitative data was collected that can be used inductively to develop a privacy management framework for PEHRs on mobile devices.

1.7.2 Research Approach

This research study followed a qualitative and interpretivist approach to research. Qualitative research focuses on an in-depth approach to describing phenomenon, and assists in gaining an understanding of underlying reasons, opinions and motivations (Wyse, 2011). An interpretivist relies on naturalistic methods, such as analysing existing texts, interviews and observations. Therefore, this study will make use of a literature review, after which critical thinking will be applied to develop the PMF. The following section will discuss the research design that will be used in this study.

1.7.3 Research Design

Yin (2014) refers to the research design as a functional plan where procedures and research methods are combined. This assists in gaining a trustworthy and valid body of data for empirically grounded analysis, theory formulation and conclusions. This study will focus on design science as a methodology; as such it is referred to as the problem-solving methodology that centres on the development and performance of artefacts for a specific problem (Hevner, March, Park, & Ram, 2004; Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

The purpose of design science is to create an innovative and purposeful artefact following an iterative design process cycle that involves building an artefact, implementing it, and then finally evaluating the outcome to determine its utility in solving the problem. There are different types of artefacts that can be constructed. These include: constructs (forms of the language used to define and communicate identified problems and their respective solutions); models (uses constructs to create an abstraction or representation of the problem and solution); methods (defines the processes required to solve the problems), and instantiations (implemented and tested systems) (Hevner et al., 2004; Vaishnavi & Kuechler, 2015). In order to provide guidance to the researcher, Hevner et al. (2004) set forth several guidelines that need to be followed, as listed in the following table.

Table 2 - Design Science Research Guidelines (Adapted from Henver et al., 2004, p. 83)

Design Science Research Guidelines		
Guideline	**Description**	**This Study**
Guideline 1 - Design as an Artefact	Design-science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.	Privacy management framework is to be developed for South African patients who use mobile devices to access personal electronic health records.
Guideline 2 - Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	There is no privacy management framework in place in South Africa to address the privacy concerns of patients that use mobile devices to access personal electronic health records.
Guideline 3 - Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The privacy management framework is to be evaluated by experts in the field of e-Health and privacy.
Guideline 4 - Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The main contribution of this study is the development of a privacy management framework to mitigate the privacy risk of South African patients who use mobile devices to access personal electronic health records.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	A qualitative and an interpretivist approach is used in this study. Expert reviews and desktop research are also used to discuss and refine the artefact of this study.
Guideline 6 - Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	Primary data (expert reviews) and secondary data (literature reviews) will be used to evaluate and refine the privacy management framework.
Guideline 7 - Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The completed thesis will be made available online. The first article was published at the Information Communication Technology and Society Conference, 2017 held in Durban. (see Appendix A)

With the incorporation of the seven research guidelines described in table 2, the following figure illustrates iterative process for the development of the privacy management framework.

Figure 2 - Development of Privacy Management Framework

The next section discusses the sample and population of this research study.

1.7.4 Sample and Population

According to Gay (1976), a research sample refers to a group of participants from an entire population to participate in a research project. The main function of a representative sample is to enable researchers to conduct their study on these participants, so that the results of the study can be used to develop conclusions that can be applied to the population as a whole (Hassan, 2013). In this study, five experts in the field of privacy and e-health were identified in order to evaluate the privacy management framework that will be developed for personal healthcare records (see Section 1.7.5.1). Furthermore, the comments from the reviewers that evaluated the article that was published at the Information Communication Technology and Society Conference, 2017 was included to improve the study. For the context of this research, an expert can range from general practitioners; published authors in healthcare privacy; to information security professionals. The following section will discuss the data collection method for this research study.

1.7.5 Data Collection

Data collection is referred to as the process by which a researcher collects information, as well as establishes the procedures for recording information to address a research problem. This information can be collected through, but is not limited to, various types of interviews, documentation, observations and surveys (Sakhti, 2013). This research study is comprised of the collection of primary and secondary data. Secondary data is referred to as data that has been previously collected by a researcher for a different purpose. Primary data is often referred to as raw and unprocessed data that is collected for specific research. (Oates, 2006). The following section will briefly discuss secondary data collection methods.

1.7.5.1 Secondary Data Collection methods

This research study will collect secondary data by means of conducting desktop research. This involved reviewing literate from previous studies such as articles from academic journals, books in both print and electronic formats, conference proceedings, relevant websites, and theories relating to this study. Electronic databases such as ACM Digital Library, Sage Online Journals, Science Direct, Springer Link and Sabinet Reference will be used to find relevant literature. Research study keywords such as 'personal health records', 'information privacy' and 'mobile device' was used as search terms. Furthermore, case studies of relevant security breaches involving medical records was utilised, as well as current and past integration of PEHR systems. The following section will briefly discuss primary data collection methods.

1.7.5.2 Primary Data Collection Methods

As mentioned previously, five experts from the field of privacy and e-Health was identified in order to evaluate the privacy management framework that was developed for personal electronic health records. The feedback received from these five experts was used to refine and adapt the proposed privacy management framework. These experts was identified during the literature review as they have published extensively in the privacy healthcare field. The experts were contacted via e-mail in order to ascertain if they are willing to participate in the study. A summary of the proposed privacy management framework was sent to these experts, and their feedback was used to further refine and adapt the framework. One round of consultations was used. Subsequently, a research article was accepted, presented and published at the Information Communication and Technology and Society Conference 2017 (Appendix A). The following section will discuss how the data will be analysed.

1.7.6 Data Analysis

Data analysis refers to how the collected data was analysed. The information gathered from primary and secondary was analysed in an inductive form. This is to determine whether the observations obtained either support or oppose the theoretical explanation presented in the research. Furthermore, qualitative data was handled differently. A thematic analysis of the data was used, as it assists in "identifying, analysing and reporting patterns within data. It minimally organises and describes your data set in detail" (Braun & Clarke, 2006, p. 79). As each expert in the field provides feedback, the information was broken down, categorised and summarised. This information was utilised to support or oppose the proposed final solution, creating an additional refinement layer for this study.

1.7.6.1 Data Trustworthiness

To ensure that the research data collected has been accurately measured, the validity of the data needs to be determined. According to Mertler (2015), the validity of qualitative data refers to the trustworthiness of this data. For this research study the credibility, dependability and confirmability of the data must be established.

Credibility refers to whether the results obtained from qualitative research are acceptable from the participants' perspective in the research (Mertler, 2015). In order to ensure the credibility of this research, triangulation was taken into consideration. Therefore, data was collected from expert reviews, legislations as well as journals, articles, book and questionnaires. This information will be checked for consistency to determine if the findings support each other.

Dependability emphasises the importance of a researcher being able to account for and describe any changes in the research setting, while noting how these changes affect the way in which the researcher directs the study (Mertler, 2015). A dependability audit can be conducted to confirm the quality and relevance of the study.

Confirmability refers to the ability of the researcher to be able to track the collected data to its source, while the logic that is used to interpret this data should be made explicit (Mertler, 2015). Therefore in order to accomplish these tasks, the researcher will archive all collected data in a well-organised format that can be made available if the research findings are opposed (Thomas, 2010). The next section discusses the proposed solution of this study.

1.8 Proposed Solution

The following figure illustrates the proposed privacy management framework (PMF), which will be thoroughly discussed in Chapter 6.

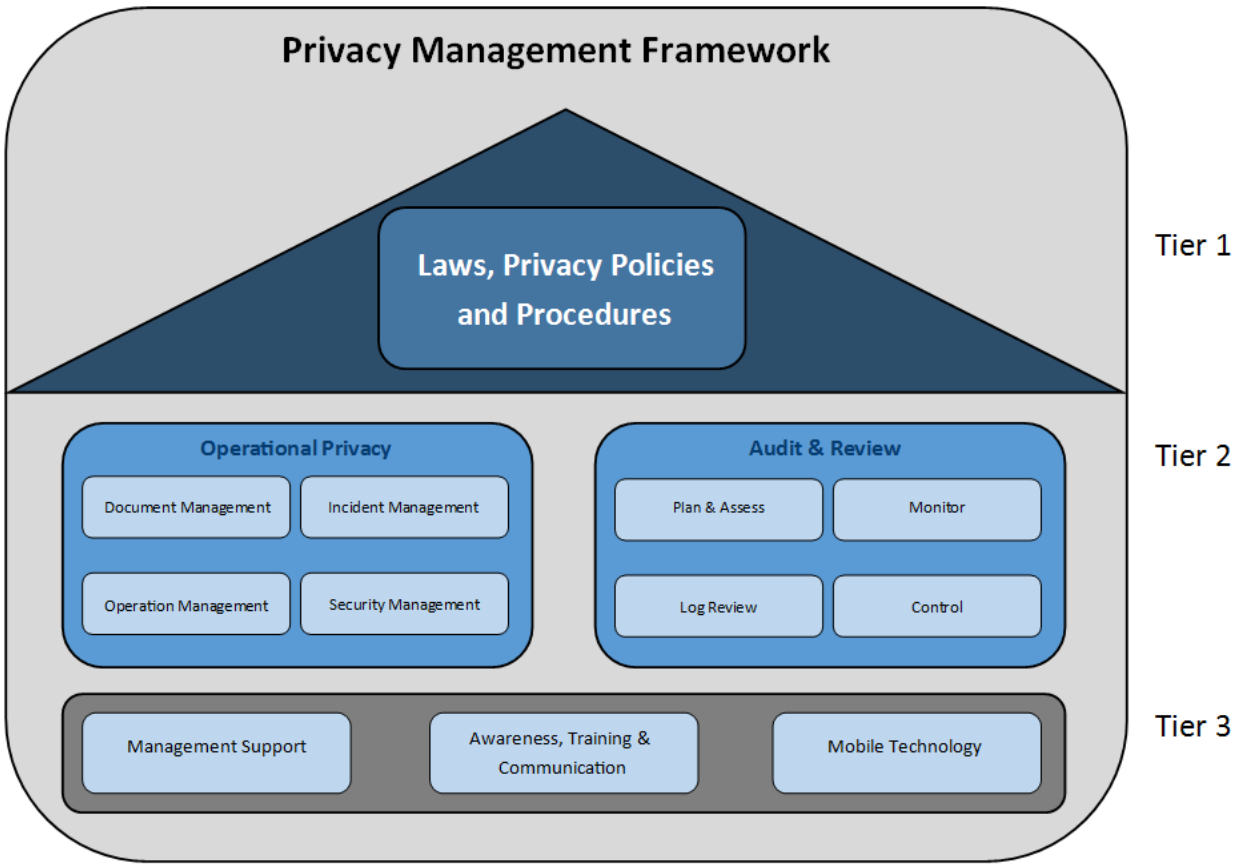


Figure 3 - Proposed Privacy Management Framework

The proposed PMF consists of 3 tiers, beginning with the top tier. The first tier relates to an organisations interpretation and understanding of data privacy laws and regulations, and in ensuring compliance with these laws. Additionally, it provides a perspective whereby an organisation is able to determine what components and requirements can be utilised to enhance information security.

The second tier refers to two support pillars to maintain the first tier. These pillars are based on elements of operational privacy, as well as auditing and reviewing. They assist in creating a privacy culture within an organisations operational policies and procedures. While audit and review focuses upon developing processes to identify and mitigate personal information breaches.

The third tier serves as the basic foundation upon which the PMF was developed. It is mainly focused with creating privacy awareness amongst healthcare providers and patients by creating: training regimes on security and privacy threats, efficient communication standards, and constant ongoing support from top level management. Organisations are able to draw references from relevant laws and regulations substantiated in the first tier to develop and adapt training regimes and standards. While the last aspect examines the use of mobile technology, and the threats that are ever present with this technology. The next section discusses the delimitations of this study.

1.9 Delimitation of the Research Study

This research project is focused on the development of a privacy management framework that can be used by healthcare providers to mitigate the privacy concerns of South African patients making use of mobile devices to access PEHRs. Therefore, the study focused upon the healthcare sector in South Africa, as well as the issues that correlate with privacy concerns of personal information. Furthermore, this study was concerned with accessing PEHRs with mobile devices and does not focus on EHRs.

1.10 Ethical Considerations

This study is in compliance with the ethical regulations stipulated by the University of Fort Hare's Research Ethics Committee. Therefore, ethical approval was applied for from the University's Research Ethics Committee (CIL031SELS01) (Appendix B).

Oates (2006) identified the following rights which will be presented to the participants (experts) during their feedback of this study:

- Wilful participation – the participants (experts) will be encouraged to participate in this research study willingly without any due force.
- Withdrawal – the participants (experts) will be allowed to withdraw from this research study at any time they feel their rights are not considered.
- Informed Consent – prior to the collection of data, the participants (experts) will informed of how the data will be collected and used, as well as any third parties that may have access to it. The participants, on the basis of this knowledge, will then either consent or refuse for their information to be used in this research exercise
- Anonymity – the participants' (experts) identity and location will be withheld unless they provide explicit permission for it to be disclosed.

1.11 Outline of Chapters

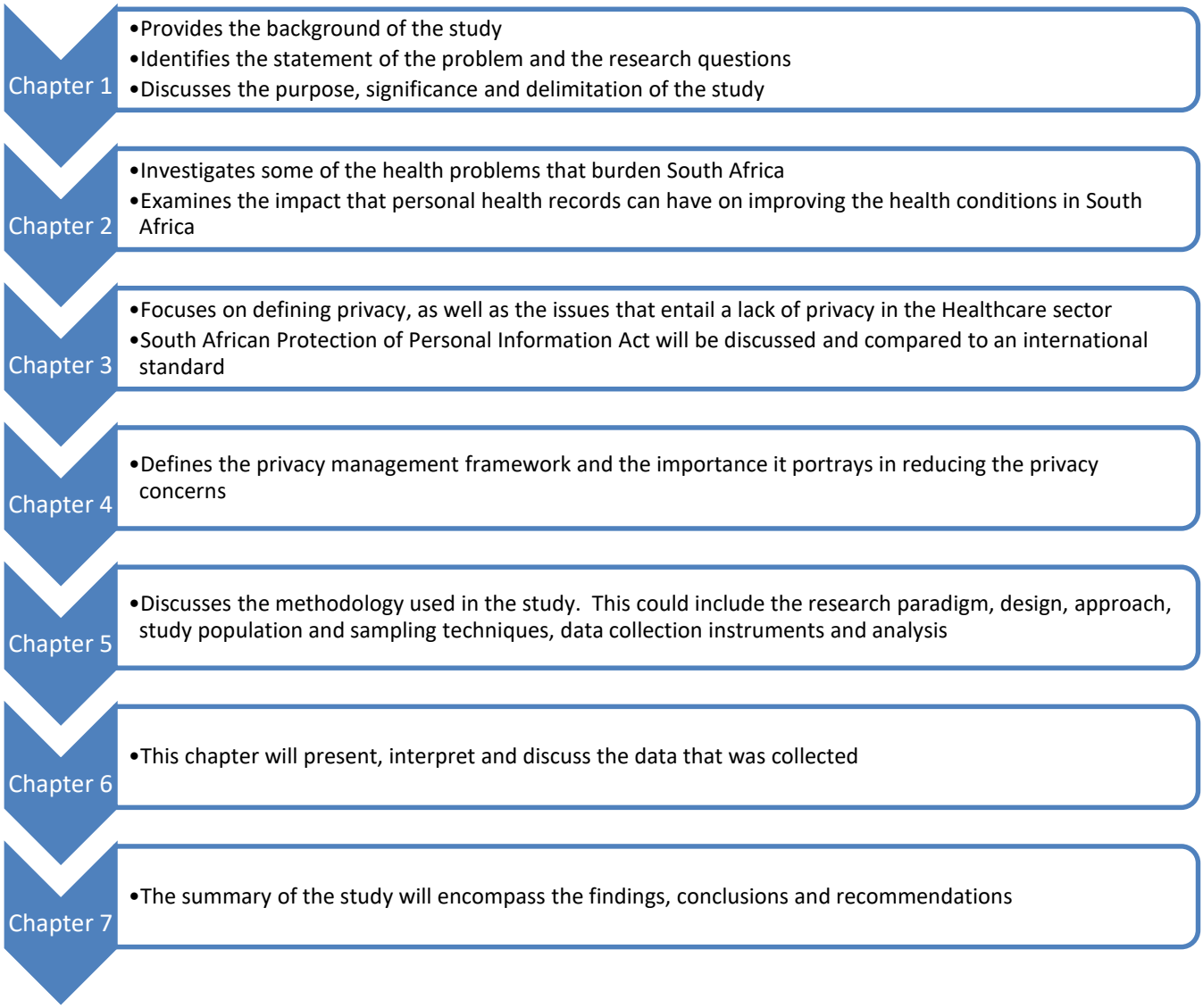
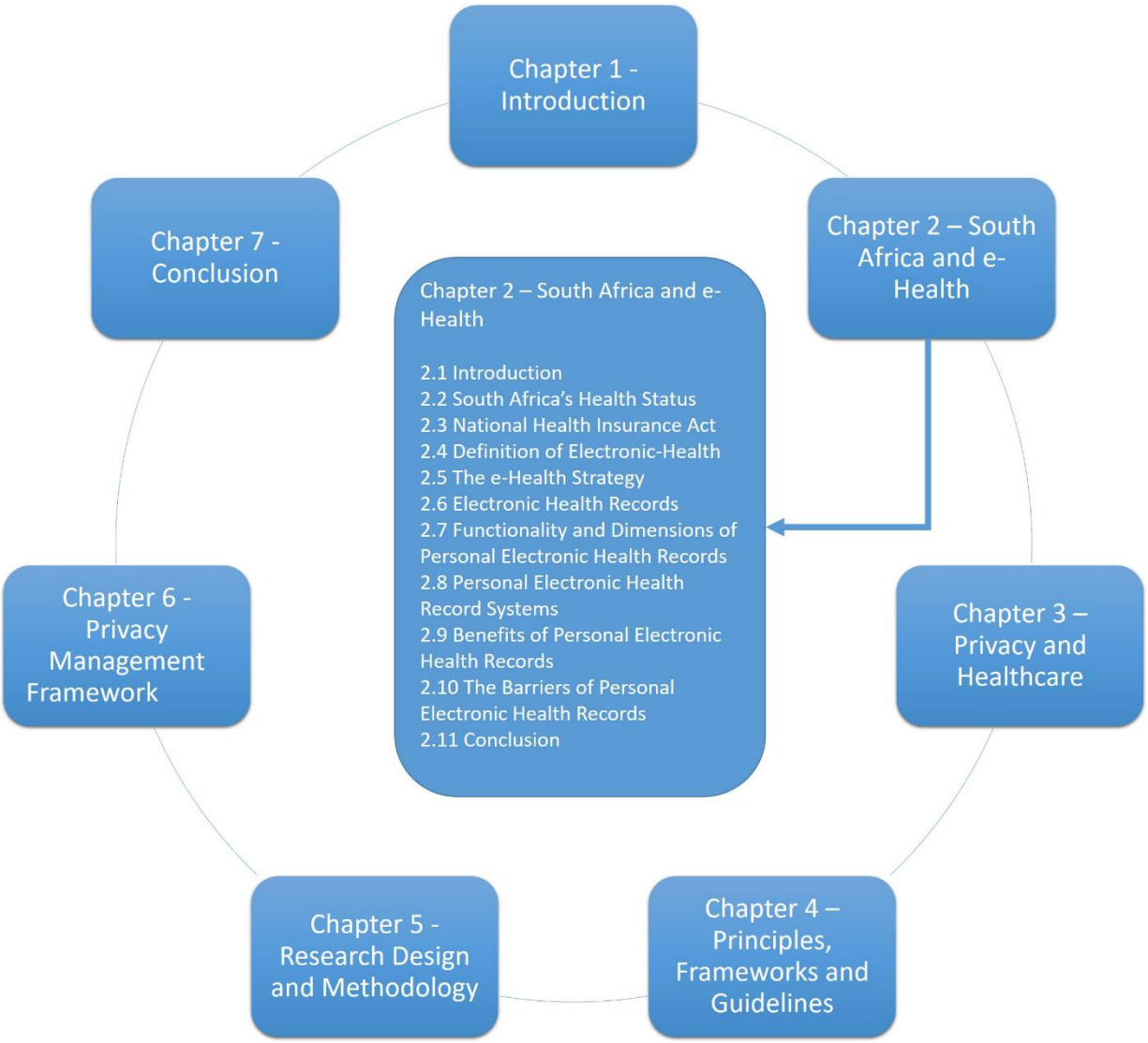


Figure 4 - Outline of Chapters

Chapter 2: South Africa and e-Health



2.1 Introduction

Technology enhanced healthcare has been prioritised by the health profession because of the decline in the health situation within South Africa. Many attribute this decline to the quadruple burden of disease. The quadruple burden of disease refers to communicable diseases such as HIV, Aids and TB; chronic diseases relating to unhealthy lifestyles; injuries resulting from trauma; and child and infant mortality rate (Yerramilli, 2015). In order to improve South Africa's current health status, the government has attempted to restructure the healthcare system making use of initiatives such as the National e-Health Strategy and National Health Insurance Act. Health and technology have been incorporated in the past to influence and improve healthcare. An important part of the e-Health initiative is the use of Personal Electronic Health Records (PEHRs). PEHRs equip patients to monitor their health information more effectively thus providing a more detailed and continuous medical history. This enables their doctors to make more informed decisions about their health care. However, although this technology has many benefits for the health care of the patient, there are barriers that can hinder its adoption.

This chapter will begin by discussing South Africa's current health status and the effect that the quadruple burden of disease has on the country. This is followed by examining the principles on which the National Health Insurance Act are built. By understanding this Act; along with the e-Health strategy of the country, a deeper understanding is created of how technology and health can be integrated. One of the parts of the e-Health is an information management system, such as an electronic record keeping system. Making use of the functionalities and purpose of the record keeping system will help to distinguish between Electronic Health Records (EHRs) and Personal Electronic Health Records (PEHRs) in the next section. PEHRs exist in various forms with various functionalities, but are able to create a centralised repository for health information. Several existing PEHRs such as Google Health and Microsoft HealthVault will be discussed and evaluated, as well as the benefits and barriers associated with PEHRs. The next section discusses South Africa's current health status.

2.2 South Africa's Health Status

South Africa's health sector ranges from basic primary healthcare that is provided by the state, to highly specialised health services in both the public and private sector. However, it has been noted that the public sector is currently under-resourced and strained in many places (Pillay-van Wyk et al., 2014). The private sector is run mainly on commercial principles and caters for the middle and high income earners whom can afford medical schemes (SA Info, 2012). Furthermore, the current private health system is considered to be biased and inaccessible to a large portion of South

African citizens. On the other hand, institutions in the public sector have endured poor administration, underfunding and a decaying infrastructure (Gaedei, & Versteegii, 2011; Pillay-van Wyk et al., 2014). One such scenario was highlighted by the Western Cape Health Department, where it was stated that 75% of its provincial citizens are without medical aid cover, relying upon the state for healthcare (Herman, 2016).

South Africa's health system is continuously being pressurized to meet the healthcare demands of its citizens, while being compounded by public health challenges that include the quadruple burden of disease (SA Info, 2012; Pillay-van Wyk et al., 2014). The quadruple burden refers to communicable diseases such as the human immunodeficiency virus (HIV), acquired immune deficiency syndrome (AIDS), tuberculosis (TB) and others. However, there are non-communicable diseases, this relates to the next burden that have a serious impact on the health status of individuals as they become older, such as hypertension, cardiovascular and chronic diseases, cancer and diabetes. The third burden of disease is injury and then trauma, which is the fourth leading cause of death among South Africans between 18-40 years of age. This is the economically active segment of the population. The last burden of disease refers to maternal and child mortality. South Africa has attempted to reduce maternal deaths, in 2009 reports by the National Health Department indicated that 189 per 100 000 births were fatal, while in 2012 and 2013 period this was reduced to 132 per 100 000 births (Cullinan, 2013). The combined effect of these communicable and non-communicable diseases has a serious impact on South Africa, doubling the death rate between 1997 and 2006 (SA Info, 2012; SA Health Department, 2015). The Western Cape Health Department has recently reported that at least 58% of South Africa's deaths were related to chronic illnesses and 36% of maternal deaths were linked to HIV and Aids (Herman, 2016).

In order to address these issues, the South African Government has responded by restructuring the healthcare system through the introduction of the National Health Insurance Act (SA Info, 2012; Pillay-van Wyk et al., 2014). The following section will discuss this Act.

2.3 National Health Insurance Act

In 2012, South Africa began to implement a health financing system known as the National Health Insurance Act (NHI). The NHI pertains to three phases; the first five-year phase focuses on strengthening service delivery, and the overall improvement of the quality in South Africa's public health sector. The second five-year phase will introduce unique identifiers linked to Home Affairs and the creation of funds to purchase primary healthcare services from public and private

providers. The final phase, will take course over a duration of four years, with focus towards ensuring the functionality of the NHI (Matsoso & Fryatt, 2013; SA Health Department, 2015). Therefore, the NHI is designed to pool resources and funds to provide access for South Africans, regardless of their socio-economic status, to affordable and quality health services (SA Health Department, 2015). Furthermore, the NHI was designed to procure services on behalf of the entire population, and to proficiently assemble and control significant financial resources. This would assist in strengthening the under-resourced public sector by improving health systems performance (Matsoso & Fryatt, 2013; Sithole, 2015).

2.3.1 National Health Insurance Principles

According to the 2015 White Paper on NHI, a more responsive and accountable health system will be implemented by the Act. This is likely to improve user satisfaction with health care, leading to a better quality of life for South Africans across all socio-economical groups. Therefore, this improvement in quality of life will assist in increasing human capital and labour productivity, while stimulating economic growth for the country (SA Health Department, 2015). In order to achieve these goals, eight principles were established for the NHI, which include:

Table 3 - National Health Insurance Act Principles (adopted from White Paper on National Health Insurance, 2015)

Principle	Description
Right to access healthcare	NHI aims to ensure that everyone has access to healthcare services. No one shall be refused emergency medical treatment
Social Solidarity	NHI will provide financial risk pooling to create cross-subsidisation, regardless of age, economic status or health status
Equity	NHI seeks to ensure a just and fair health system for all, where the greatest health needs will be provided with timely access to health services
Healthcare as a Public Good	Healthcare will not be treated as a commodity, but rather as social investment
Affordability	Healthcare services will be procured at a reasonable cost that recognises the need for sustainability within the context of the country's resources.
Efficiency	Healthcare resources will be distributed and utilised in a matter that emphasises value for money
Effectiveness	NHI aims to ensure that the health system meets acceptable standards of quality while achieving positive health outcomes
Appropriateness	The healthcare system will adopt an innovative service delivery models tailored to the needs of the population, and delivered at appropriate levels of care

From these principles, a comprehensive healthcare system will be achieved through accredited and contracted public and private providers. Furthermore, an extensive amount of focus and resources are being directed at health promotion and prevention services at a community and household level (SA Health Department, 2015).

In order to realise the implementation of the NHI system, technology will have to be incorporated and expanded in the public health care system. South Africa has launched their National e-Health Strategy in 2012, seeking to embrace Information and Communication Technologies to develop and expand current healthcare systems (Matsoso, & Fryatt, 2013). Section 2.3 will discuss the e-

Health Strategy further, while the following section will examine the concept of e-Health, and how technology and healthcare have been integrated.

2.4 Definition of Electronic-Health

Health and technology have been known to be incorporated so as to influence healthcare worldwide, and with the use of online health information, the internet has become an influential source of knowledge (Currie & Seddon, 2014; Xiao, Sharman, Rao & Upadhyaya, 2014). The application of electronic health (e-Health), a term that depicts the use of computers, information or communication technologies for some aspects of healthcare, is viewed as an essential part to solving the problems facing healthcare systems (van Gemert-Pijnen, Wynchank & Ossebaard, 2012). Electronic health is able to assist in the structural reforms needed to ensure the sustainability of health systems while creating and securing access to services (Ross, Stevenson, Lau & Murray, 2015). The World Health Organization (2013), states that e-Health will portray an important role in reinforcing national health systems and services, while reducing costs in providing information for governmental decision and policy making. Electronic health has emerged due to the rapid adoption of technology, and advancements in mobile health (m-health). Mobile health refers to the use of mobile devices in the practise of medicine and public health (Adibi, 2015).

South Africa and Nigeria were identified in 2015 as two prominent countries with the highest mobile device ownership in Africa, where up to 90% of people in these countries possess a mobile device (Pew Research Centre, 2015). Sahu, Grover and Joshi (2014) note that within these developing countries, mobile technology has been able to improve the health outcomes for chronic diseases such as diabetes, hypertension and heart diseases through interoperability between various systems, networking and communications, remote monitoring, as well as security and privacy mechanisms. The following section discusses the concerns with e-Health.

2.4.1 Concerns with e-Health

However, despite the potential benefits of e-Health, there are several issues that hinder its overall adoption. These concerns include:

- The lack of a sufficient Information and Communications Technology (ICT) platform on which to develop a national health information infrastructure;
- Managerial concerns with establishing sufficient administrative structures and mechanisms to ensure accountability, transparency and effective leadership;

- Delays in increasing the development of high-priority e-Health solutions;
- Attracting private sector investments;
- Developing and training essential human resources; and
- Supporting secure electronic information exchange across geographical and health sector boundaries.

(Esmaeilzadeh, Sambasivan, & Kumar, 2010; World Health Organization, 2013; Ozair et al, 2015)

Research studies have shown that any financial, legal, ethical or social barriers towards e-Health occur at both an organisational and individual level (Currie & Seddon, 2014). These can stem from either a user's lack of awareness of the benefits; a low level e-Health literacy rate; interoperability issues with regard to communication and data storage and lastly, security concerns with data (Currie & Seddon, 2014; Ross et al., 2015). Identifying and understanding the barriers as well as the facilitators are crucial to developing strategies and interventions to advance the adoption of e-Health (Ross et al., 2015). South Africa has attempted to address these concerns by developing and introducing its own e-Health Strategy (Currie & Seddon, 2014). The following section will discuss this strategy.

2.5 The e-Health Strategy

In order to ensure the effective monitoring of healthcare service delivery and overall performance of South African health systems, a suitable and functional health information system is required. This system must be able to provide real time information for decision-making processes. From an international perspective, ICT has emerged as an essential mechanism to govern healthcare and creates an innovative solution to service delivery (e-Health Strategy, 2012; Fortuin & Naidoo, 2015). However, South Africa's health information system has been characterised by discontinuity and a lack of co-ordination. The prevalence of the lack of interoperability between systems creates a significant hindrance to healthcare delivery (e-Health Strategy, 2012). In order to reach these goals, ten strategic priorities were established, alongside six domains of healthcare quality set forth by the Institute of Medicine (e-Health Strategy, 2012). The following section will discuss these priorities and domains.

2.5.1 e-Health Strategy Priorities and Domains

In order to efficiently implement the e-Health Strategy plan in South Africa, ten priorities need to be co-ordinated (e-Health Strategy, 2012; Masilela, Foster, & Chetty, 2013).

Table 4 - e-Health Strategic Priorities (Adapted from e-Health Strategy, 2012; Masilela, Foster & Chetty, 2013)

Strategic Priority	Description
1 - Strategy and Leadership	Emphasises the importance of political, executive and clinical leadership to reach successful recognition.
2 – Stakeholder Engagement	Engagement by all stakeholder groups is required to help mobilise support, recognise any opportunities and priorities, as well as to manage and mitigate risk.
3 – Standards and Interoperability	Standards are an essential base for successful implementation. There is also a requirement for national standards for procurement of hardware and software such as data structures, clinical coding, and messaging and electronic health records.
4 - Governance and Regulation	Electronic health affects stakeholders across a multitude of domains such as personal health, healthcare provision, ICT and management. This emphasises the need for an efficient governance structure.
5 – Investment, Affordability and Sustainability	Before commencement of an e-Health project, financing must be procured and protected over the duration of the project. This also requires appropriate planning to identify the benefits so that value for money and affordability are balanced.
6 - Benefits Realisation	Develop a benefits realisation plan which specifies health outcome benefits expected at a local level for all e-Health interventions.
7 - Capacity and Workforce	Human resource capital is recognised as an integral part of a successful e-Health deployment. A workforce is needed to innovate, develop, deploy and manage all e-Health interventions such as health information and health management information systems. This is achieved by developing career paths, as well as implementing training and skill retention strategies.
8 – e-Health Foundations	The strategy is to be deployed in a step-wise manner, with focus on four areas which will provide the foundations for all other e-Health activities. This includes infrastructures and connectivity, patient registration, facilities and providers, and a basic electronic health record.
9 - Applications and Tools to support Healthcare Delivery	There is a wide range of digital applications tools available to support and improve healthcare delivery. These include business health intelligence, electronic health record systems, electronic content management, surveillance systems, as well as decision support and knowledge management.
10 - Monitoring and Evaluation of the e-Health Strategy	Continuous and consistent monitoring and evaluation are required to determine the performance of the e-Health Strategy. This ensures that objectives are met, and provides input for future strategies and procedures.

The ensuing aim of the e-Health Strategy is to provide clear guidelines to elevate South Africa's current public health sector into an integrated and well organized patient-based information system. The e-health Strategy also focuses on the interoperability between systems to improve the effectiveness of clinical care and enable patient mobility (e-Health Strategy, 2012). All of the priorities stated in Table 4 are essential for enabling the implementation of the NHI (e-Health Strategy, 2012). Furthermore, the e-Health Strategy is based upon taking an incremental approach to development, as such improving upon what already exists in the public and private sectors, and filling the gaps wherever necessary. It aims to improve current infrastructures and connectivity, increase the basic ICT literacy rate and develop human resources as well as affordability planning (Masilela, Foster, & Chetty, 2013). Various and widely used e-health technology include information management systems such as an electronic health records, which will be discussed in the following section.

2.6 Electronic Health Records

Electronic record keeping systems can be classified into two different categories. The first category is called an electronic health record (EHR). An EHR can be described as a comprehensive electronic collection of a patient's health history that is maintained and controlled by healthcare personnel (Healthcare Information and Management Systems Society, 2014). EHRs can contain information such as diagnoses, immunisation dates, treatment plans and laboratory results (Garret & Seidman, 2011; Weiss, 2016). These EHRs therefore allow for the acquisition, distribution and storage of patient data; while utilizing computerised decision support systems, such as diagnostic support and alerts as well as communication systems such as telecommunication and information resources (Ross et al., 2015). They are considered to be a real-time based functionality that permits instant availability and ubiquity as required by healthcare personnel. However, a patient's health history is deemed confidential and the information submitted in an EHR should only be shared with other authorised healthcare providers and organizations (Kemp, 2016; Els & Cilliers, 2017). The next section will discuss personal electronic health records.

2.6.1 Personal Electronic Health Records

The evolution of the electronic record is called a personal electronic health record (PEHR). A PEHR is described as a health record where a patient's health data and information is managed and controlled by the patient (Tang, Ash, Bates, Overhage & Sands, 2006). Price, Bellwood, Kitson, Davies, Weber & Lau (2015) note several uses of PEHR that include:

- Accessing own Health Data – a patient can access available clinical records or view lab results;
- Accessing Health Information – a patient can access protocol information or self-management information in a central knowledge base;
- Recording Personal Health Data – PEHRs can be utilized to track and record subjective experience data or objective data related to a patient's condition over time;
- Receive Personal Decision Support – PEHR data can create an initiative for evidence-based reminders and alerts for a patient, increasing self-management;
- Plan Care – a patient can proactively set personal goals and targets for his/her healthcare;
- Self-Manage Care – PEHRs can be utilized in a patient's everyday decision-making about their care management;
- Communication with Care Team – patients are able to engage and support members of a circle of care, either virtually or face-to-face through direct communication or data sharing; and
- Communication with Support Group – patients are able to utilize PEHRs as a secure platform to engage in communication with informal members of a care team or community for support.

PEHRs have the capability to reduce medical errors and enhance the monitoring of health conditions. This is achieved by creating a centralised repository which enables an effective communication pathway between patients and healthcare providers as relevant information can be shared (Krist & Woolf, 2011; Bouri & Ravi, 2014). As patients are able to take ownership of monitoring their own health information more effectively, their health status may improve. However, the information contained in a PEHR does not replace the legal records of a healthcare provider (Givens & Cordary, 2012). The following section will discuss the several types of PEHRs that exist.

2.6.1.1 Types of Personal Electronic Health Records

Steele, Min and Lo (2012) state that PEHRs can exist in various forms, dependent upon where and how they are stored. These include Local, Remote Server-Based or Hybrid PEHRs. The following sections will discuss these variations of PEHRs.

A Local PEHR refers to storing data locally, through either a paper or device-based system, and is characterised by the fact that internet connectivity is not required to access the information (Steele

et al., 2012). With a paper based PEHR, the patient keeps his/her information in folders collected from different physicians. When the patient makes use of a device-based PEHR, a patients' record is stored on a portable device, with the most common being a USB device or mobile device (Maloney & Wright, 2010; McClain & Thompson, 2010). However, this may require specific architectural infrastructure that relies on the type of device used (Steele et al., 2012).

Remote server-based PEHRs refer to storing the data through an internet connection on either a web-based, proprietary application or cloud-based servers (Botts et al., 2011; Simons et al., 2005; Tang 2006). This allows for access to the information anywhere or anytime, as long as there is an active internet connection. Therefore, with this type of PEHR there is no guarantee that patients will have a real-time-based accessibility to their healthcare data, as it highly dependent on a continuous and stable internet connection (Salfner, Lenk, & Malek, 2010). A healthcare provider is usually the entity that manages this type of PEHR (Steele et al., 2012).

Lastly, a Hybrid PEHR is a combination of local and remote PEHRs enabling data to be duplicated on both a local storage device as well as a remote server. This type of PEHR creates increased flexibility and accessibility to the data, as it is likely to endure infrastructural vulnerabilities and unexpected system failures (Steele et al., 2012). The following section will provide a more detailed comparison between these PEHRs by examining the architectural foundations.

2.6.2 Architectural Comparison between PEHRs approaches

There are various architectural approaches to PEHRs, each with its own advantages and disadvantages. From the different variations of PEHRs discussed in the previous section, there are different architectural infrastructures that need to be investigated. This relates to network connectivity; data storage locations and device; concomitant hardware and software; and fundamentally the reliability of currently implemented infrastructure (Steele et al, 2012). This section will discuss these notions further.

2.6.2.1 USB-based Portable Storage

A portable storage-based PEHR that utilizes USB devices, provides patients with the convenience of being able to carry their healthcare data while travelling (Maloney & Wright, 2010). Therefore, as mentioned in the previous section 2.6.1.1, a USB-based device can contain a local-based PEHR.

However, there is a limitation to this attribute, and that is dependent upon whether or not the USB device has been physically damaged or not. If the device sustains no damage, then the stored

PEHR can be accessed with minimum requirements, as only a computer with a USB interface is required (Steele et al., 2012). Furthermore, these portable storage devices can provide patients with privacy and security for their PEHR as there is no network connectivity, removing the element of an intrusion (Kharrazi et al., 2012). Occasionally these storage devices themselves are not able to be readily interconnected with other systems without concomitant devices (Maloney & Wright, 2010). This restriction can prevent data from being integrated with other data sources as there is no standardization or interoperable interfaces between them. Furthermore, in order to sustain the continuity of care, the PEHR is required to be maintained over the patient's lifetime. With the concept of this being a localized and standalone PEHR, the patient may be responsible for performing maintenance and ensuring the data is backed up (Steele et al., 2012). The next section will discuss mobile device-based PEHRs.

2.6.2.2 Mobile Device-based

Mobile devices with computing capability and wireless internet connectivity can be utilised as a local data repository to access existing online PEHRs (Keckley & Chung, 2010; Bouri & Ravi, 2014). Additionally, a mobile device is considered to maintain a hybrid PEHR with is flexibility. As such, mobile device-based PEHRs are able to provide real time access to healthcare data without a fixed network connection and concomitant devices creating more portability (Mosa, Yoo & Sheets, 2012). This leads to the ability of patients being able to dynamically provide healthcare professionals with data on demand. However, the ability to provide real time data or dynamic data management may require a more accurate authorship control, in order to ensure the reliability of data (Steele & Min, 2010; Kharrazi et al., 2012). Furthermore, mobile devices may be connected to an unpredictable wireless environment, creating an opportunity for non-trusted mobile devices to access and jeopardize the privacy and security of healthcare data. Additionally, there may be restraints to data sharing with third parties, as interconnectivity may not be facilitated for mobile devices (Keckley & Chung, 2010; Steele & Min, 2010). Although mobile device-based PEHRs can be automatically upgraded by manufacturers, there are concerns about the stability, fault tolerance and computational capability of the PEHR application, as well as the reliability of wireless connections. Similar to the storage-based PEHR, the patient can be responsible for safeguarding data to minimize loss (Steele et al., 2012). The following section will examine remote server-based PEHRs.

2.6.2.2.1 Remote Server-based

Remote server-based PEHR can be categorised into two architectures, specifically a web-based or a cloud-based PEHR, which will be discussed in the following subsection. With a web-based

PEHR, a web browser is required to access data or the PEHRs are stored on a proprietary application server that requires dedicated client software to access the data (Steele et al., 2012). Furthermore, most server-based PEHRs are commonly interconnected with systems used by specific healthcare providers (Xhafa, Li, Zhao, Li, Chen, & Wong, 2015). As mentioned in the previous section, portable devices that contain a wireless network connectivity enable patients to access, manage and update healthcare data in real time by connecting to these servers. However, accurate authorship is required to confirm the reliability of the data provided (Steele et al., 2012; Kharrazi et al., 2012). In comparison to standalone PEHRs, web-based applications can improve the standardization of data exchange and representation (Silva, Rodrigues, de la Torre Díez, López-Coronado & Saleem, 2015). Unlike portable storage and mobile devices, server-based PEHRs are usually maintained and upgraded by the organisations. With regard to data backup and recovery, this is dependent upon the systems' capabilities. Furthermore, the quality and speed of ubiquitous telecommunication infrastructure portrays an integral part upon the adoption of this PEHR (Steele et al., 2012). The next section will discuss cloud-based PEHRs.

2.6.2.2.2 Cloud-Based

A cloud-based PEHR portrays another form of remote server-based PEHR. It requires a continuous network connectivity that supports a reliable ubiquitous technological environment, by which patients and healthcare providers are able to access PEHRs through wired or wireless computing devices such as mobile devices. Cloud-based PEHRs increase the agility and resilience of accessing, processing and storing patient healthcare (AbuKhousa, Mohamed, & Al-Jaroodi, 2012; Steel et al., 2012). In contrast to the dedicated servers provided by third parties or healthcare providers, cloud-based PEHR utilize virtual, dispersed servers and store data through interconnected networks (Sarwar, & Khan, 2013). However, with the distributed storage of healthcare data, there is a greater concern with the privacy and security of this data (Schweitzer, 2012). The following section will examine the concept of a hybrid PEHR.

2.6.2.3 Hybrid

A hybrid PEHR is able to provide unmatched availability and flexibility to healthcare data, as the patient can access their information either locally or online. This type of PEHR can enhance the limitations of data integration and sharing, fault tolerance and data recovery (Steele et al., 2012). Subsequently, network connectivity is a fundamental element for hybrid PEHRs, but in comparison to a remote server-based PEHR, an omission or fault may not severely affect data accessibility and availability. Furthermore, depending on the situation at present different methods can be used to access the healthcare data (Steele et al., 2012). In order to ensure the reliability and

integrity for both locally and remote stored data, appropriate policies need to be implemented, therefore enabling a consistent and secure access control to a patient's healthcare data (Kraan, Piggott, van der Vegt, & Wisse, 2015). Without this insurance of reliability and integrity between local and remote PEHRs, there is no guarantee of data consistency which may result in critical medical errors being made (Steele et al, 2012).

From the discussion in the previous sections, it is clear that PEHRs can become a main pillar of patient healthcare, as it represents an information system in which all medical data of the patient can be assembled. As most PEHRs are Internet based, it creates a user-driven approach to higher data quality (Sunyaev & Chornyi, 2012). Patients are interested in obtaining the best treatment for themselves, thus patients have to be interested in creating the best database to evaluate their state of health (Sunyaev, 2013). The next section will discuss the nine dimensions for PEHRs and the significance of functionality.

2.7 Functionality and Dimensions of Personal Electronic Health Records

Functionality is considered an important key point of PEHRs, due to the fact that these records are comprised of various components to assist patients and healthcare providers in improving the decision-making process and healthcare of the patient (Krist & Wolf, 2011; Steele et al., 2012). These components relate to the capture, storage and integration of a patient's healthcare data. Furthermore, these functional capabilities can affect the overall adoption by patients, as well as other implications such as improving the standard of healthcare and safety; empowering decision-making and reducing healthcare costs (Kellermann, & Jones, 2013; Monkman & Kushniruk, 2013). However, the functional requirements of PEHRs depend on the architectural design and its infrastructure (Steele et al., 2012). As such, van der Westhuizen (2012) described nine dimensions and requirements needed to be satisfied in order to ensure that PEHRs are considered functional and useful. The following table 5 briefly examines these dimensions.

Table 5 - PEHR Dimensions (adopted from van der Westhuizen, 2012)

Dimension	Requirement
Accuracy	Any information captured must be done so correctly by implementing tools that prevent human error.
Apomediation	PEHRs should educate patients and assist them in capturing records with a sense of understanding. These patients must also have the ability to interact with the physicians.
Auditability	PEHRs must contain audit logs to track any access, modifications and deletions. It should also support non-repudiation.
Availability	PEHRs need to be accessible by the patient and physician at all times. Emergency access must also be enabled.
Completeness	In order for PEHRs to be considered complete, it must contain basic personal information, physician visits, and diagnoses, as well as information such as diet and exercise logs, health insurance information.
Confidentiality	PEHRs are only to be accessed by authorised parties.
Integrity	No unauthorised modifications or deletions, while any authorised modification is to be tracked by audit logs.
Interoperability	This refers to the ability of PEHRs to operate with other health systems to interchange health information.
Privacy	A patient must have the ability to allow or deny access to his/her PEHR.

Before 2012, patient-accessible PEHRs were almost non-existent in South Africa. If patients wanted to manage and store their own information they would have to rely on international vendors such as the failed Google Health Program or the current Microsoft HealthVault. The following section briefly examines the commercial PEHRs systems that are available.

2.8 Personal Electronic Health Record Systems

There are currently numerous PEHR systems available, each dependent upon its own business models, design approaches, licensing and even functionality (Sunyaev, 2013). This section will examine some of these systems, by first looking at Google Health.

2.8.1 Google Health

Google is known to be the world market leader as an internet search engine, among business and other expansions. However, in 2008 Google attempted a personal health information service known as Google Health, but by 2011 this service was discontinued (Sunyaev, 2013). There were several factors that contributed to Google Health failing. These were related to the lack of functionality in terms of communication and convenience, such as being able to send secure messages and scheduling appointments with healthcare providers (Chase, 2011; McGee, 2011). Furthermore, privacy concerns arose, as consumers feared whether their health information was made public in Google Search (McGee, 2011; Spil & Klein, 2014). Another major factor, which contributed to Google Health failing, was insufficient third-party support for data integration across multiple sources and applications (McGee, 2011; Spil & Klein, 2014). The following subsection will discuss Microsoft's perspective on a PEHR.

2.8.2 Microsoft HealthVault

In comparison to Google Health, Microsoft's HealthVault's greatest advantage is interoperability and functionality (Sunyaev, 2013). It is able to connect with an array of devices, gadgets and applications, allowing data to be imported automatically into one location (Duffy, 2014).

HealthVault creates peace of mind for its consumers, as their health information is governed by Microsoft's corporate privacy policies, which entails four core principles (HealthVault, 2015):

- All health records created in the HealthVault are controlled by the consumer;
- The consumer determines what information goes into a health record;
- The consumer determines who can see and use their health information on a case-by-case basis; and
- Health information is not used for commercial purposes.

The next subsection focuses on the South African PEHRs known as HealthID and HealthSpace.

2.8.3 Health ID

In 2012, Discovery Health launched a personal health record system application known as HealthID in South Africa (Erasmus, 2014). As the healthcare professionals that a patient consult

are often from separate practices, there is a lack of co-ordination and a limited sharing capacity of critical health information that would enable these professionals to make better informed decisions about their patient's health care (Mayo, 2012). Discovery aims to reduce the inefficiency of administrative burdens as well as the paperwork involved in the process, by creating a centralised point of information for its members. Therefore, through HealthID, patients are able to conveniently access their medical history, diagnoses, visitation schedules and electronic prescriptions in one place (Discovery, 2012; Mayo, 2012). An essential aspect of HealthID is the protection of a patients privacy rights, as such only prescribed and relevant doctors are able to register and access HealthID (Discovery, 2012). Additionally, the information being accessed is not stored on the device being used, but rather on Discovery's Health Servers, such as remote based PEHR. Once the doctor logs out, all access is revoked (Discovery, 2012; Mayo, 2012). The following subsection discusses another South African PEHR.

2.8.4 My HealthSpace

Similar to Discovery's HealthID, another South African system was developed by HealthSpace, referred to as *My HealthSpace*. My HealthSpace is a free PEHR system that enables patients to store their medical history online; search for health professionals; view health professional's notes, as well as access laboratory results through a secure web-based portal (My HealthSpace, 2012). The functionalities are limited, and as it is a free service the development, data storage and exchange costs are subsidised by visible advertising on the website (My HealthSpace, 2012). The following sections will discuss some of the benefits and barriers of PEHRs.

2.9 Benefits of Personal Electronic Health Records

This section will discuss some of the benefits associated with using PEHRs. This is achieved by providing a perspective from the different invested stakeholders, namely the patient, the healthcare provider and lastly from an economic viewpoint.

2.9.1 Patients Perspective

Firstly from a patient's perspective, there are several aspects which can be discussed (Tang et al., 2006; Kim & Nahm, 2012; Steele et al., 2012):

- Behavioural Changes – PEHR can improve a patient's health behaviour with regard to dietary changes, regular exercising regimes, reduced tobacco consumption and an improvement in medication compliance;

- Chronic Disease Management – patients using PEHRs are able to better manage and track their disease to see changes through consultations, as well as create an early intervention for when a problem emerges;
- Enhanced Communication – integrated data can provide for a more complete view of relevant health information for both the patient and healthcare provider;
- Enhanced Patient Satisfaction and Safety – patients experience better satisfaction with regard to how they manage their own health information, as well as have access to an array of credible health information when needed;
- Improved Efficiency and Ease of Use – patients are able to access health information with minimal effort and resources, as well as supporting multiple-user views for a user-friendly interaction; and
- Patient Empowerment – PEHRs can empower patients by allowing them to access and manage their own personal health information, creating more engagement in the health process and improving health outcomes.

The following subsection will discuss the benefits associated with a healthcare provider's perspective.

2.9.2 Healthcare Providers Perspective

From a different viewpoint, healthcare providers provide a more in-depth perspective (Tang et al., 2006; Etzioni, 2010; Kim & Nahm, 2012; Steele et al., 2012):

- Access to Patient Data in Emergencies – PEHRs creates an ease of access to patient information in emergency situations, increasing survivability rate of the patient;
- Enhanced Communication – as PEHRs removes the need for face-to-face communication and appointments, creating an increase in communication between the healthcare provider and patient, creating and on-going connection between the two;
- Information Backup – patients that keep a copy of their PEHR, reduce the impact of data becoming damaged or lost;
- Information Sharing – PEHRs are able to be shared amongst various healthcare providers and facilities which the patient visited.
- Quality of Healthcare and Decision Making – the healthcare provider has access to better health history, resulting in a better understanding of the patient, as well as reducing the chances of repeating any unnecessary medical treatments and diagnoses; and

- Economically – PEHRs are able to reduce healthcare costs, such as reducing management, medication and wellness program costs.

Despite these various benefits of PEHRs, there are barriers that need to be examined. These will be discussed in the following section.

2.10 The Barriers of Personal Electronic Health Records

This subsection will discuss the barriers affecting PEHRs (Tang et al., 2006; Steele et al., 2012; Vance, Tomblin, Studney & Coustasse, 2015):

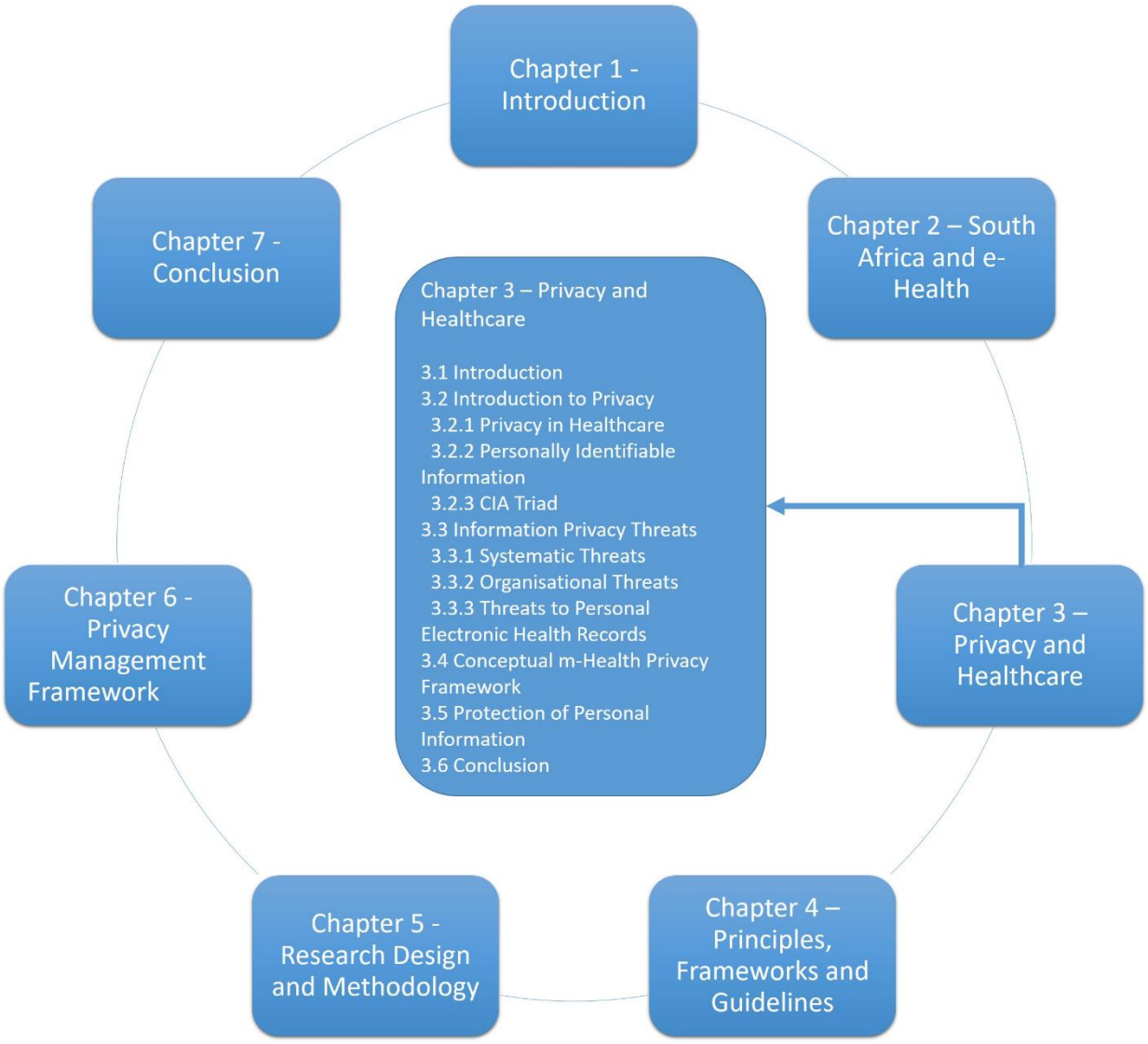
- Data Integrity and Accuracy – healthcare providers often worry about the dependability of the data entered by patients, due to the lack of their medical background. This could result in data being rendered unusable or the healthcare provider not utilizing the information;
- Data Privacy and Security – a major concern for patients is about who has access to their sensitive information once it has been recorded online, as not all parties have ethical or legal obligations to respect the privacy of a patient;
- Digital Divide and Illiteracy – PEHRs has presented a problem to individuals that are illiterate; do not know how to use a computer or do not have access to a computer;
- Interoperability – at times patients and healthcare providers are unable to share information across organisations, as the logistics of implementing transparent interoperability across different systems is a difficult task;
- Legal Concerns – healthcare providers are concerned with the repercussions of relying and acting upon PEHRs, which may hold inaccurate information;
- Usability – patients with cognitive or physical disabilities may recognise the need to use a PEHR, but are unable to do so without assistance; and
- Workload and Compensation – healthcare providers are apprehensive about an increase in workload, and not being compensated for the amount of time spent updating PEHRs.

The national e-Health strategy guide can be highlighted as a contributor towards the development of the first tier of the PMF, which entails laws, policies and procedures. Additionally, there are concepts with the e-Health strategy guide, which assisted in developing the third tier of PMF, foundational support. This refers to managerial support as well as awareness, training and communication.

2.11 Conclusion

This chapter has discussed and examined South Africa's current health status and the impact of the quadruple burden of disease, as well as how the government aims to improve this status through the incorporation of the National Health Insurance Act and National e-Health Strategy. Through the understanding of e-Health, the functionality of Electronic Health Records and Personal Electronic Health Records were established. The functionalities of each PEHR were discussed and compared while also looking at the benefits and barriers to its adoption from patients and a healthcare provider's viewpoint. The following Chapter will discuss the privacy and security issues related to PEHRs.

Chapter 3: Privacy and Healthcare



3.1 Introduction

The previous Chapter discussed some of the aspects that affect South Africa's current health status, as well as how government seeks to improve this situation through the implementation of the National e-Health Strategy and the National Health Insurance Act. Alongside this Strategy and Act, the benefits and barriers of PEHRs were identified.

Health information is deemed to be private and sensitive information to a patient, therefore controls must be in place to protect a patient's privacy. This Chapter is focused upon the privacy issues and threats that can affect a patient, the healthcare providers or organisations. This chapter begins by first examining what privacy is, and the different types of privacy, followed by privacy in healthcare. Within this section, personally identifiable information (PII) and the aspects of CIA Triad are discussed. This leads into the identification of information privacy threats, and the threats to PEHRs. The final section compares and contrasts the international Conceptual m-Health Privacy Framework and the South African Protection of Personal Information (PoPI) Act. The following section will discuss privacy.

3.2 Introduction to Privacy

Privacy is known to be an attribute by which various new developing technologies are critiqued, especially technology that involves personal information and data (Finn, Wright, & Friedewald, 2013). According to Privacy International (2016), "Privacy is a fundamental right, essential to autonomy and the protection of human dignity" (p.54). It allows for individuals to establish boundaries in which to protect themselves from unnecessary interferences in their daily lives, thus limiting who has access to their bodies, locations and communications (Finn, Wright, & Friedewald, 2013; Privacy International, 2016).

Finn, Wright and Friedewald (2013) identify several categories of privacy which relate to:

- Privacy of the Person – individuals have the right to keep body functions and characteristics private;
- Privacy of behaviour and action – individuals have the right to keep sensitive information such as sexual orientation and habits, as well as political and religious views private;
- Privacy of communication – involves the prohibition of the interception of an individual's communication including telephonic or wireless communications;
- Privacy of data and image – concerns with making sure that an individual's data is not available to unauthorised individuals and organisations;

- Privacy of thoughts and feelings – individuals have the right not to express or share thoughts and feelings;
- Privacy of location and space – individuals have the right to move about in public or semi-public spaces without being identified, monitored or tracked; and
- Privacy of association – individuals have the right to associate with whomever they wish without being monitored.

From a healthcare perspective, information privacy is a continuously developing issue. Technology constantly introduces new challenges to maintaining the confidentiality, integrity and availability of healthcare data (O'Brien, 2010). With the integration of PEHRs, there is an increased need for information exchange between patients, healthcare providers and organisations. Furthermore, as information is it stored and transmitted in bulk, there is an increase in the possibility of it being targeted by malicious outsiders and organisations (O'Brien, 2010; Finn, Wright, & Friedewald, 2013). Therefore it is essential that the privacy categories mentioned previously are understood and entwined into an organisational culture. The following section will discuss the impact of privacy in healthcare.

3.2.1 Privacy in Healthcare

Privacy is viewed as an important part of governing a patient-physician relationship, as patients are required to share information in order to facilitate a correct diagnosis and treatment (Appari & Johnson, 2010). Furthermore, the sharing of a patient's personal information may only occur within the limitations specified by a patient. Therefore, the physician may forward the information to be captured electronically (Boucher, 2013). However, patients may also choose not to disclose sensitive information such as psychiatric behaviour or HIV status as it may lead to a social stigma. When information is withheld, inaccurate and incomplete data is entered into a healthcare system, and any subsequent data used for research or public health reporting is invalid (Nass, Levit & Gostin, 2009; Appari & Johnson, 2010).

The benefits of privacy for patients include the ability to avoid exploitation or embarrassment. Examples of such situations include identity theft, fraud, blackmail, discrimination and harassment. As such, they exemplify exploitations by identity thieves, employers, health insurance companies and even governments (O'Brien, 2010). Historically, the most common and known ethical commitment taken by physicians is The Hippocratic Oath, translated from Greek approximately 400 B.C:

"Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private." (Anonymous, n.d).

This Oath means that is it a physician's duty to ensure a patient's privacy rights are honoured, even though in situations the physician may share the information with other practitioners if they deem it in the best interest of the patient (O'Brien, 2010). A doctor may consider breaching the patient's privacy if they feel the patient is a danger to himself/herself or if the underlying condition will determine how the patient is treated by another doctor. Governments do mandate health information privacy from a legal perspective, ensuring breach notifications, increased security enforcement and the introduction of auditing among health care providers (O'Brien, 2010). South Africa is no exception with Section 3.5 elaborating further on this. Security violations may lead to the disclosure of sensitive business data of an organisation, including financial data, intellectual property and even patient's health information. This may inevitably have disastrous effects for the organisation such as loss of income, reputation and competitive edge (Appari & Johnson, 2010; O'Brien, 2010).

As mentioned in the previous section, information about individuals has become more accessible through the advancements of technology. These individuals depend upon many forms of personal identifiers in order to differentiate between each other (Connelly, 2011). Subsequently, defining and protecting personal identifiable information (PII) has become an essential component of privacy (Narayanan & Shmatikov, 2010). The following section will discuss PII further.

3.2.2 Personally Identifiable Information

Jessup and Neal (2009) refer to PII as information that can be used to locate or identify individuals. It consists of different categorised information that includes educational history, employment information, demographics, financial history and, more importantly, medical information (Jessup & Neal, 2009; Narayanan & Shmatikov 2009). Therefore, PII is widely defined to consist of, but not be limited to, information that relates to (McCallister, Grance & Scarfone, 2010):

- Names, Identifying Number, e-Mail and Physical Address, Telephone Numbers;
- Race, Ethnic or Social Origin, Language, Cultural Beliefs, Gender, Sex, Sexual Orientation, Marital Status, Pregnancy, Physical and Mental Status, Disabilities;
- Medical, Financial, Employment and Criminal History;
- Personal and Religious Views;

- Biometric Information, Blood Type; and
- Information Identifying Personally Owned Property – Vehicle Registration.

This private and sensitive information is often used by individuals in an attempt to combine several separate pieces of information to compromise the individual's identity. The information is easily obtainable through online databases and social networks (McCallister, 2010). There are, however, policies and regulations in place that attempt to restrict organisations from inappropriately sharing any form of PII data, while also imposing requirements for sufficiently protecting such private information (Connelly, 2011). Section 3.4 and 3.5 will discuss these policies and regulations further, while the following discuss the CIA Triad.

3.2.3 The CIA Triad

The CIA Triad is an information systems security model that was developed as a tool to assist organisations and individuals in implementing information security measures. As such, the primary goal of information security is to ensure the confidentiality, integrity and availability of all private and sensitive information held by an organisation. The Triad provides safety controls for paper or computer-based systems, such as web-browsers or communication (Gibilisco & Rouse, 2013). By creating a safe and secure environment, the organisation can ensure that a patient's information is protected from any form of manipulation by both authorised and unauthorised individuals. Many organisations and regulatory mandates manage how specific types of information, including sensitive medical and financial data, must be processed, stored and transmitted (Gibilisco & Rouse, 2013). The CIA Triad is able to provide a high-level structural foundation for assisting with privacy and compliance regulations of private information (Ihonvbere, 2010). A benefit of the CIA Triad is that it is utilised as a guiding concept in establishing policies and procedures, as well as to benchmark information systems and implementations (Perrin, 2008; Gibilisco & Rouse, 2013).

3.2.3.1 Confidentiality of Data

The confidentiality aspect of the Triad aims to ensure that critical data is only accessible to individuals who have sufficient and appropriate access. Therefore, from a healthcare perspective, there needs to be a limitation within the organisation that restricts the access to PII, as well as preventing the disclosure of such information to unauthorised individuals or organisations (Perrin, 2008; Ihonvbere, 2010; Gibilisco & Rouse, 2013). The following section examines the integrity aspect of the Triad.

3.2.3.2 Integrity of Data

Integrity relates to the protection of organisational and individual information from being altered. This provides an assurance that the data will not inappropriately be altered, either accidently or deliberately, as well as assuring the trustworthiness of the stored information. This aspect further states that any information must have originated from the intended entity or individual. Therefore any information that is transmitted, recorded and entered into a system should reflect actual, reliable and correct records (Perrin, 2008; Ihonvbere, 2010; Gibilisco & Rouse, 2013). The next section discusses the last aspect of the Triad, availability.

3.2.3.3 Availability of Data

Most modern organisations are highly dependent upon a functioning information system, as such availability aims to guarantee that any critical organisational information is readily and constantly available, but only to authorised individuals. Similar to the other aspects, it may be affected by technical problems and natural or human phenomena. Additionally, as the relative risks associated with these categories are dependent upon their context, the general assumption is that humans are always the weakest link in a system. This assumption revolves around each individual's ability and willingness to use a data system securely within the limitations of private information (Perrin, 2008; Ihonvbere, 2010; Gibilisco & Rouse, 2013).

However, despite the implementation of these aspects, the CIA Triad may at times be taken for granted or overlooked within these organisations (Gibilisco & Rouse, 2013). The following section will examine some of the information privacy threats experienced.

3.3 Information Privacy Threats

Appari and Johnson (2010) noted two broad categories of identifiable threats to information privacy. This refers to organisational and systematic threats. Organisational threats often stem from inappropriate access to patient data through the abuse of access privileges or a vulnerability being exploited. A systematic threat arises from an individual that is a part of the information flow chain that exploits information beyond its intended use (Kotz, 2011; Avancha et al, 2012). The following section will discuss organisational threats in further detail.

3.3.1 Systematic Threats

As mentioned previously, with systematic threats patient privacy is vulnerable to individuals with legal and privileged access to patient information. It is these individuals within the information flow chain that pose the greatest threat (Appari & Johnson, 2010; Jouini, Rabai& Aissa, 2014).

3.3.2 Organisational Threats

Organisational threats may present themselves in various forms, from the first being employees who have access to sensitive patient information without a valid reason, and the second from outside threats such as hackers that attempt to steal or disrupt patient information in the database. Different threats pose different levels of risk for an organisation, which is dependent upon individual components such as accessibility, motive, resources and technical capabilities (Appari & Johnson, 2010; Kotz, 2011). The following table examines how these components can be categorised into several classifications:

Table 6 - Threat Classification (adapted from Appari & Johnson, 2010)

Component	Description
Accidental Disclosure	Patient information may be accidently disclosed by healthcare personnel to others.
Data Breach by Insider	Healthcare personnel may access patient information and transmit it to outsiders for economic profit or revenge
Data Breach by Outsider (Physical Intrusion)	Outsiders may enter the facility through coercion or forced entry, and gain access to the systems and patient information
Data Breach by Outsider (Network Intrusion)	Outsiders such as patients, hackers or former employees may access an organisations network to gain access to patient information, or render system inoperable.
Insider Curiosity	Healthcare personnel with access privileges view patient information out of curiosity or for their own purpose.

While the privacy threats presented in Table 6 focus on patient information being shared or breached while it is stored in the organisation's database, there is also an additional threat for patients that make use of their mobile devices to access their health information. Avancha et al. (2012) derived three common privacy threats that share similar traits, but relate to mobile devices and the use of PEHRs. The following section will discuss these threats further.

3.3.3 Threats to Personal Electronic Health Records

The first threat identified relates to identity, whereby patients may misplace their mobile device, lose their mobile device due to theft or unintentionally share their identity credentials with others. These actions enable an unauthorised individual to access patient's confidential information, breaching their privacy (Avancha et al., 2012). Additionally, individuals might use a patient's identity to obtain medical services, resulting in financial repercussions for the patient (Johnson, 2009; Taitsman et al., 2013). One such example occurred at the Howard University Hospital in Washington, where a medical technician utilised his/her position to illicitly gain access to confidential patient information. The technician eventually began to sell this information over a 17-month period before being apprehended (Ozair, Jamshed, Sharma, & Aggarwal, 2015). From another perspective, most modern mobile devices contain content sharing applications, as well as Bluetooth and Wi-Fi connectivity. These features may leave a patient vulnerable to hacking and malware.

The second threat identified relates to the access of PEHRs. Patients may mistakenly modify their own data incorrectly if the access-controls of the PEHR are too permissive. This can also be related to the design of a mobile device, such as screens being too small, or a patient does not fully understand how to use the device. While on the other end of the spectrum, a patient may intentionally modify their personal information to gain reimbursement through financial fraud or malice (Dixon, 2006; Taitsman et al., 2013; Els & Cilliers, 2017).

The last privacy threat relates to the disclosure of the information within PEHRs, which includes data at rest and in transit. Both these types of information are vulnerable to attack. As such, packet sniffing is an example that allows an unauthorised individual the ability to capture data that is being transmitted. Another concept is the man-in-the-middle, whereby an attacker secretly relays and possibly alters information that is being transmitted (Kaufman, Perlman, & Speciner, 2002; Els & Cilliers, 2017). This information may be disclosed inadvertently by a patient or an individual with access to the information, allowing data disclosure beyond the intended purposes (Avancha et al., 2012). The disclosed information may be utilised for financial gain or to humiliate the patient (Appari & Johnson, 2010). Examples of the threats mentioned above include an external contractor to the Howard University Hospital who had downloaded more than 34 000 patient files to his mobile device, before it was stolen (Ozair et al, 2015). A more recent incident occurred in August 2016, where 42 health data breach incidents occurred within the United States, involving close to 3.6 million patient records. It was noted that 43-percent of these breaches were

linked to insider threats that involved accidental and intentional wrongdoing, 29-percent were related to hacking, and the remaining percentile were related to theft and loss (Landi, 2016).

These occurrences indicate that safeguards do fail at times. As such, compliance and legislation are a necessity for healthcare organisations. The following section will discuss and compare the Conceptual m-Health Privacy Framework against the South African Protection of Personal Information Act.

3.4 Conceptual m-Health Privacy Framework

The Conceptual m-Health Privacy Framework was developed upon the requirements of various international security policies and standards such as the Health Insurance Portability and Accountability Act (HIPAA), the Markle Common Framework (CF) and Office of the National Coordinator for Health Information (ONC). However, the Conceptual m-Health Privacy Framework was designed to be implemented for a mobile health platform, but does not extend to PEHRs (Avancha et al., 2012). The following section will discuss the principles that form the Conceptual m-Health Privacy Framework.

3.4.1 Openness and Transparency

The first principle of the framework, Openness and Transparency, relates to the responsibility of the healthcare provider to inform patients what information has been collected about them; the purpose of the information as well as who has access to this information (Markle Common Framework, 2008). Furthermore, it stipulates that the patients should be informed by the healthcare provider, regarding how they may obtain access and control of the information gathered (Markle Common Framework, 2008; HIPAA, 2010). Additionally, any polices and technologies being employed should be disclosed to the patient (ONC National Framework, 2008).

3.4.2 Purpose Specification

The second principle, Purpose Specification, relates to the reason for which the personal information is being collected which should be stipulated at the time in which the information is collected (Markle Common Framework, 2008). Additionally, once the information is collected, it should not be used for any purposes not previously disclosed to the patient (ONC National Framework, 2008). However, this is exempted when specific situations arise where it is important that information be disclosed to avoid any harm to the patient (Kim, McGraw, Mamo, & Ohno-Machado, 2013).

3.4.3 Collection Limitation and Data Minimisation

The Conceptual m-Health Privacy Framework states that the collection of personal health information should only be collected by the healthcare provider for the intended purposes and be obtained in a fair and lawful manner, with the consent of the patient (Markle Common Framework, 2008). Furthermore, the collection and storage of this information be limited to only the information required for specific purposes (Markle Common Framework, 2008).

3.4.4 Use Limitation (Transitive)

The Use Limitation principle outlines the regulations related to the use of patient information once it is collected. As such, a patient's information should not be disclosed or made available to third parties by the healthcare provider, as well as not being used for other than the specified purposes (HIPAA, 2010). However, this can be exempted with the patient's consent (Markle Common Framework, 2008).

3.4.5 Individual Participation and Control

The Individual Participation and Control principle aims at providing the patient with the ability to control the access to their personal information (HIPAA, 2010). The healthcare provider should make the patients aware of who is storing what information about them and how it can be used (Markle Common Framework, 2008). Furthermore, the patients should be well informed about how this data is being collected and disclosed (ONC National Framework, 2008).

3.4.6 Data Quality and Integrity

Data Quality and Integrity focuses on certifying that the stored patient information is accurate, complete and updated timeously (HIPAA, 2010; Markle Common Framework, 2008; ONC National Framework, 2008). Taitsman, et al (2013, p. 978) state that, "Incorrect information can infiltrate the beneficiary's medical record and corrupt later medical decision-making". Furthermore, healthcare providers should provide patients with a timely means of disputing the integrity of their personal information, by being granted access to correct the erroneous information (Markle Common Framework, 2008; ONC National Framework, 2008). However, accountability should be present in the process of altering the information (Kotz, 2011).

3.4.7 Security Safeguards and Controls

Security Safeguards and Controls relate to placement of administrative, technical and physical safeguards, by healthcare providers to protect patient information both physically and electronically (HIPAA, 2010; ONC National Framework, 2008). These safeguards minimise the

risk of loss, unauthorised access, misuse or destruction of information (Markle Common Framework, 2008).

3.4.8 Accountability and Remedies

Accountability and Remedies refer to the integration of accountability, enforceable by the healthcare provider in control of the patient's information (HIPAA, 2010). As such, any administrator or provider involved must be accountable for the processing of any information (Laursen, 2013). Furthermore, remedies should be prepared to be implemented in the situation of a privacy breach (Markle Common Framework, 2008).

3.4.9 Patient Access to Data

Patient Access to Data stipulates that patients should be able to obtain their health records and be permitted to update their records by the healthcare provider (ONC National Framework, 2008). By permitting a patient to access his/her record, addresses any delays or lack of information exchange amongst the healthcare providers and the patient (Patel & Siminerio, 2014). However, this information should be marked with a unique identifier to ensure the integrity and relevance contained within the record (Markle Common Framework, 2008; HIPAA, 2010).

3.4.10 Anonymity of Presence

The last principle applies to circumstances where medical sensing devices are used in the collection of patient data, whilst the patient is in his/her natural environment making this unique to m-Health (Avancha et al, 2012). As such these sensing devices are able to monitor a patient's health continuously without interfering with his/her daily activities (Mare, Sorber, Shin, Cornelius & Kotz, 2014). The following section will discuss South Africa's Protection of Personal Information Act.

3.5 Protection of Personal Information

Kingwill (2016) stated that the South African legislative environment is considered to be constantly changing and developing. The observation was verified when the South African Government introduced the Protection of Personal Information Act (PoPI) of 2013, amongst others. This act attempts to address the privacy and security concerns in the collection of personal information, but is not designed for a mobile health environment (Townsend & Ncube, 2013; Botha & Booi, 2016). The following section will examine the PoPI Act further.

South Africa has introduced the Protection of Personal Information Act of 2013 (PoPI), to regulate the processing of personal information. Although this Act is not specifically designed to protect privacy in healthcare information, the PoPI Act prescribes that personally identifiable information (PII) contained in a patient's medical records must be private and secure (Calaguas, 2013). As such, the purpose of the act is to give the effect of a constitutional right to the privacy of an individual and to safeguard any personal information when processed by a responsible party (SA Justice Department, 2013). However, as stated by Tuyikezea and Pottas (2005, p.11), "being compliant with all legal requirements does not guarantee privacy and security protection of health information". The PoPI Act is centralised upon eight core information privacy principles which all related parties need to comply (SA Justice Department, 2013).

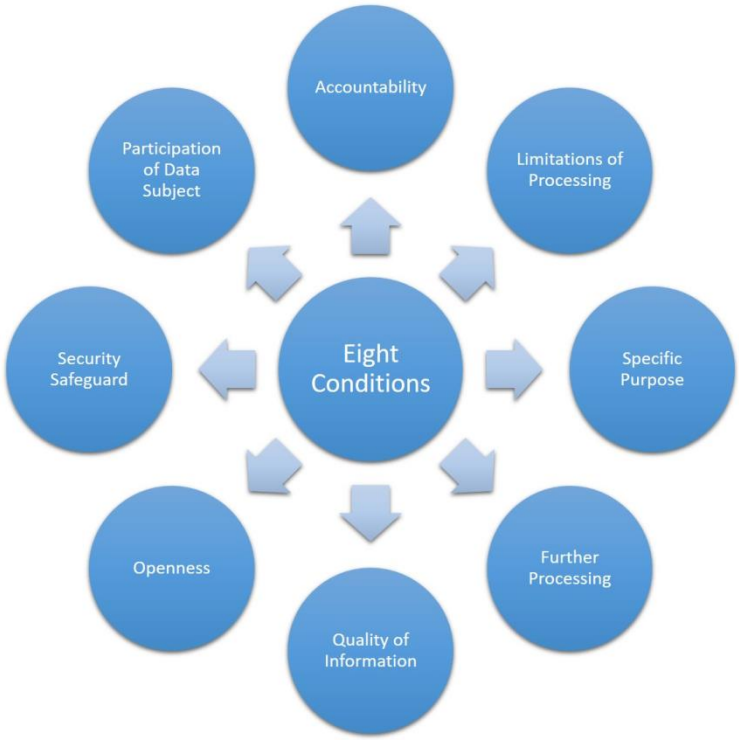


Figure 5 - Eight Core Principals of PoPI (Protection of Personal Information BIll, 2013)

Figure 5 illustrates the eight core principles of the PoPI Act, while the following section will discuss these principles in more detail.

3.5.1 Processing Limitation

The first principle that will be discussed refers to Processing Limitation. Only with consent of the individual or data subject should personal information be processed (Basson & Van Zyl, 2014). However, this process pertains to a lawful and reasonable manner that does not infringe upon the privacy of the patient. Additionally, despite the general prohibition of processing of sensitive information, healthcare providers and medical schemes may process information as needed for the

proper treatment for administrative purposes (Dinnie & Malherbe, 2014). However, this information may only be processed if the purpose of its collection is adequate, relevant and not excessive. Subsequently, personal information required must be collected directly from the data subject unless this information has been deliberately made public by the individual (SA Justice Department, 2013).

3.5.2 Purpose Specification

Purpose Specification states that personal information must be collected for explicitly defined and legitimate reasons. Additionally, the data subject must be made aware of the purpose for the collection of his/her information as well what this information encompasses (Basson & Van Zyl, 2014). Furthermore, the records of personal information must not be retained any longer than required for achieving its purpose. Once a responsible party is no longer authorised to retain these records, they must be destroyed or de-identified as soon as reasonably practicable (SA Justice Department, 2013).

3.5.3 Further Processing Limitation

Similar to Processing Limitation discussed previously, the further processing of personal information must be compatible with the purpose for which the information was initially collected (Basson & Van Zyl, 2014). To determine whether further processing is compatible with the purpose of the collection, the responsible party must take into account the nature of the information concerned (Dinnie & Malherbe, 2014). Additionally, the manner in which the information was collected and the consequences that further processing will have for the data subject must be considered. However, there are circumstances which deem further processing incompatible, such as mitigating a serious threat to the life of the data subject or another individual (SA Justice Department, 2013).

3.5.4 Information Quality

The next aspect of the PoPI Act relates to the quality of information. As such, a responsible party, such as the health care organisation, must take reasonable and practicable steps to ensure that the personal information processed is accurate, reliable, and complete (Basson & Van Zyl, 2014). Additionally this information should be updated when necessary to avoid any misrepresentations or distortions (SA Justice Department, 2013).

3.5.5 Openness

Openness entails a responsible party maintaining the documentation of all processing operations under its responsibility. If personal information is collected, then the data subject is to be made aware of what information has or not been processed as well as the purpose and source of the information (Basson & Van Zyl, 2014). Furthermore, dependent upon whether or not the supply of information by data subject is voluntary or mandatory, the responsible party is to inform the individual of any consequences for failing to provide information (SA Justice Department, 2013).

3.5.6 Security Safeguards

Security Safeguards refers to the security measures to be employed by responsible parties in ensuring the confidentiality and integrity of personal information within their possession (Basson & Van Zyl, 2014). Additionally, if any person acting under authority processes the information, it should be performed in a manner that regards the information as confidential and must not be disclosed, unless by law. This notion is of particular importance to healthcare providers who process information on an individual's behalf (Townsend & Ncube, 2013). Taking the appropriate technical and organisational measures, which are dependent upon the situation entailed, assists in preventing the unauthorised access or loss of information (Dreyer & Mandim, 2014). However, if an unauthorised access occurs, the appropriate parties need to be informed immediately to mitigate any resulting consequences (SA Justice Department, 2013).

3.5.7 Data Subject Participation

A data subject, only with adequate proof of identity, may request for the correction or deletion of outdated personal information which holds any misleading or inaccurate information (Basson & Van Zyl, 2014). It is, therefore, dependent upon the responsible parties to allow the data subject to access and manage their personal health information (Dreyer & Mandim, 2014; SA Justice Department, 2013).

3.5.8 Accountability

The last principle defines the obligation of the responsible party to ensure that all conditions mentioned previously are complied with from the time the information is gathered up to and including the time of destruction (Basson & Van Zyl, 2014). Furthermore, these compliance standards are monitored, so as to respond to any privacy complaints and breaches (Calaguas, 2013; Dreyer & Mandim, 2014). Therefore the obligation is on the responsible party to ensure accountability for the information processed (SA Justice Department, 2013). The following table

which is depicted in Chapter 1 compares how the PoPI Act correlates with the guidelines of the conceptual framework for m-Health privacy.

Table 1 - Comparison of the South African Protection of Personal Information Act and Conceptual Framework for m-Health Information Privacy Principles (adapted from Dala & Venter, 2015)

Conceptual Framework for m-Health Information Privacy Principles	**PoPI Requirement Addressed**
Openness and Transparency	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 6**)
Purpose Specification	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 3** and **4**)
Collection Limitation and Data Minimization	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 2, 3** and **4**)
Use Limitation (Transitive)	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 2, 3** and **4**) - and Chapter 6: Prior Authorisation
Individual Participation and Control	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 8**)
Data Quality and Integrity	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 5**)
Security Safeguards and Controls	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 7**)
Accountability and Remedies	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 1**) - deals with Accountability - while (**Condition 7**) - provides provision that a patient is to be alerted in the event of a data breach. Furthermore, Chapter 5: Supervision - introduces the information regulator which will be the privacy enforcement regulator.
	For the implementation of this principle, there is no specific reference to a privacy management framework. However, Chapter 11: Offences, Penalties and Administrative Fines - makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintaining good policies, procedures and practices to protect personal information.
Patient Access to Data	Yes - Chapter 3: Conditions for Lawful Processing of Personal Information - (**Condition 6** and **8**)
Anonymity of Presence	Not addressed in the PoPI Act

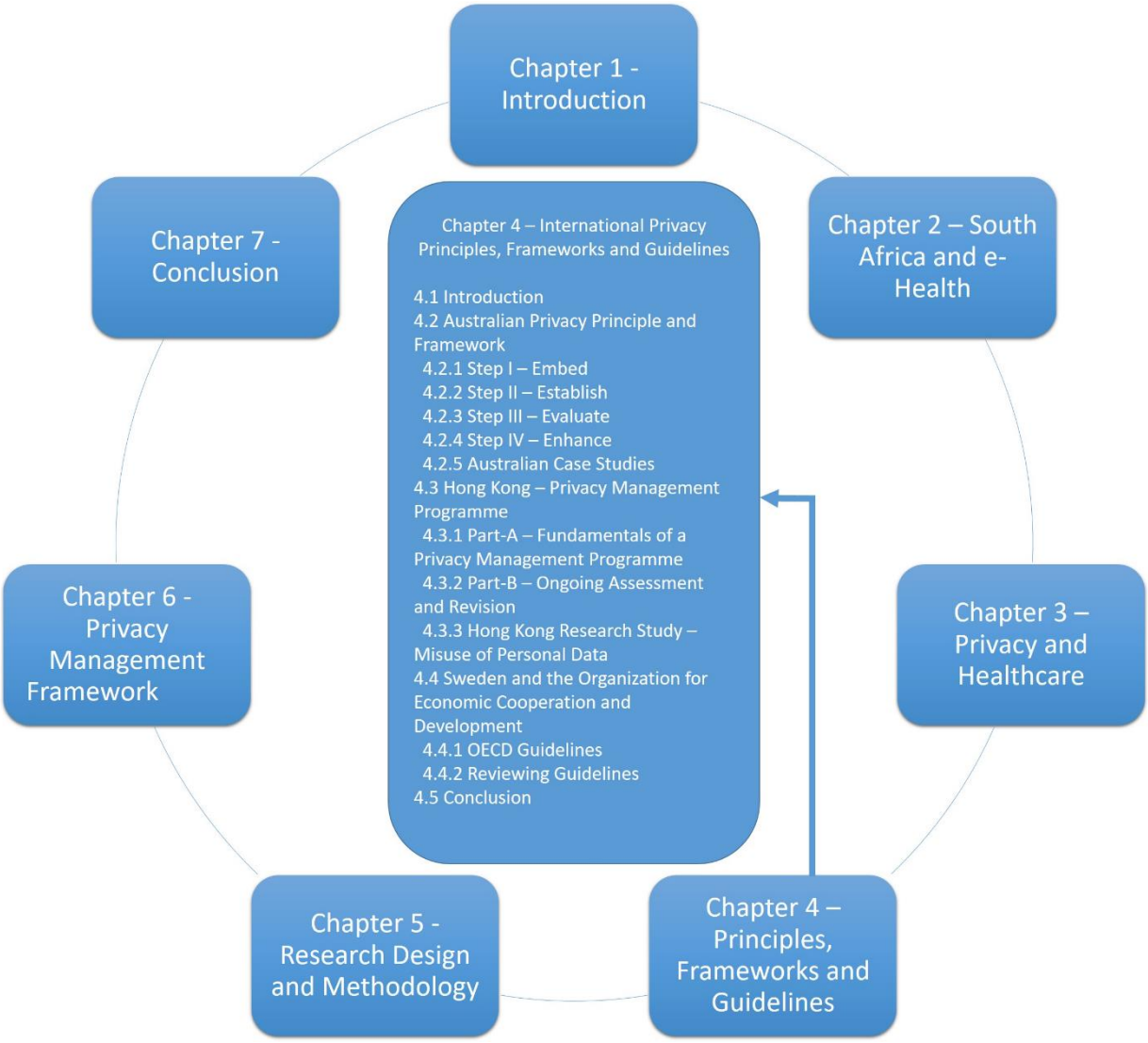
As seen in Table 1, there are similarities present between the Conceptual m-Health Privacy Framework and PoPI Act. However, there is an exception present which refers to the lack of a privacy management framework.

The PoPI Act portrayed an important role in developing the PMF, as it contributed to establishing several aspects of the PMFs support pillars. This refers to document, incident as well as operation management. While in conjunction with South Africa's National e-Health Strategy Guide, which was discussed in Chapter 2, and the Conceptual m-Health Privacy Framework, the PoPI Act assisted in a further refinement of the first tier of the PMF. Lastly, awareness, training and communication elements of the PMF were highlighted and established through an understanding of PoPI and the conceptual framework.

3.6 Conclusion

This chapter has discussed and examined the importance of privacy, especially a patient's privacy with regard to his/her PII. As technology continuously evolves, there are continuous challenges to maintaining the confidentiality, integrity and availability of healthcare data. Through the introduction of the CIA Triad, an ethical, legal and organisational perspective of this privacy is substantiated. Lastly, through the comparison of the Conceptual m-Health Privacy Framework and the PoPI Act, the absence of a privacy management framework was inferred, which will be discussed in the following chapter.

Chapter 4: International Privacy Principles, Frameworks and Guidelines



4.1 Introduction

The previous chapter was focused upon privacy issues and threats that can affect a patient and healthcare providers or organisations. This chapter will be evaluating and discussing the concept and purpose of a privacy management framework, as well various countries across the globe, which maintain some form of a privacy management framework for the protection of information privacy. This includes both private and public privacy regulators, such as Australia, China and Sweden. These three countries were chosen as a basis for the evaluation as each come from different economic, political, and healthcare orientated backgrounds

The Australian Government has developed a privacy management framework making use of a four step guideline process. These steps refer to the embedment of a privacy culture to enable organisational compliance; establishing a robust and effective privacy process; evaluating these processes to ensure continuous effectiveness and lastly enhancing responses to privacy issues (Australian Information Commissioner, 2015). A year earlier, the Chinese Government also created similar in-depth privacy framework guidelines, but the focus of their framework was on creating organisational commitment and implementing programme controls. Characteristics of their framework refer to the integration of a privacy culture throughout an organisation with top-management commitment; a continuous risk assessment analysis; policy training and education for those that interact with personal data; communicating privacy concerns and continuously assessing and reviewing the privacy framework (Hong Kong's Office of the Privacy Commissioner for Personal Data, 2014). Sweden currently has its own Personal Data Act, but also form part of the Organization for Economic Cooperation and Development (OECD). This necessitates understanding the eight basic data protection principles of the OECD Guidelines (OECD, 2013). The next section will discuss these case studies in more detail.

4.2 Australian Privacy Principle and Framework

The Australian Privacy Principles (APP) was extended in order to meet ongoing privacy compliance obligations. The APP refers the application of several principles to handle and manage personal information. This refers to the creation of a Privacy Management Framework (PMF) from the Office of the Australian Information Commissioner (OAIC). The PMF is considered to be a four step guideline process. As mentioned previously, these steps refer to the embedment of a privacy culture to enable organisational compliance; establishing a robust and effective privacy process; evaluating these processes to ensure continuous effectiveness and, lastly, enhancing responses to privacy issues (OAIC, 2015). Correspondingly, each step offers a list of commitments that organisations are encouraged to comply with, however, these commitments are

dependent upon the organisation's scope, resources and business model (von Dietze, 2015). Figure 6 illustrates these steps, which will be discussed further in the following section, beginning with embedment of a privacy culture.

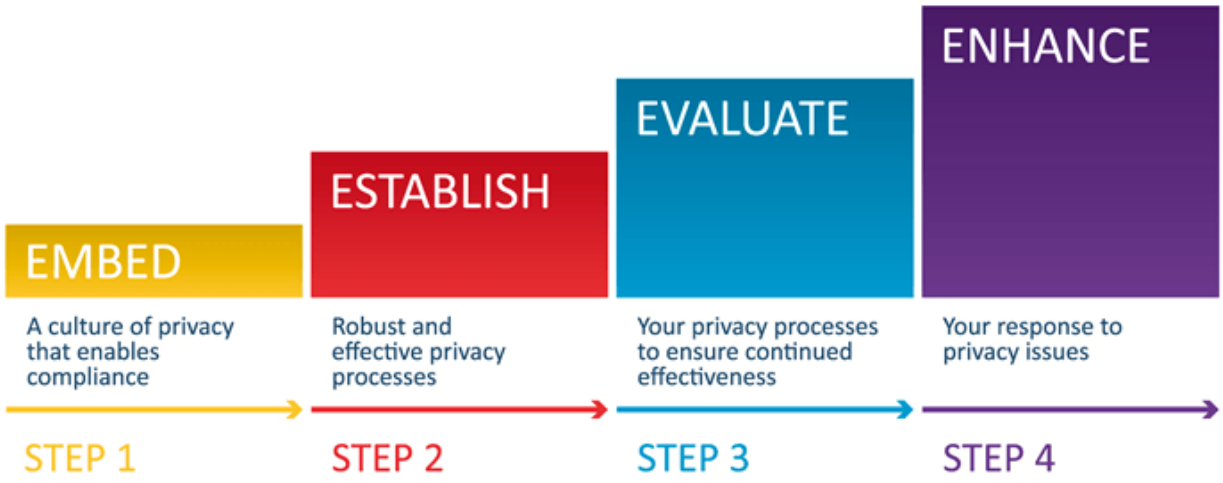


Figure 6 - Privacy Management Framework Steps (OAIC, 2015)

4.2.1 Step I - Embed

As demonstrated in figure 6, the first step refers to embedding a privacy culture within a healthcare organisation. As such, a "good privacy management stems from good privacy governance", (OAIC, 2015, p.3). It is essential that leadership and governance creates a privacy culture which values the importance of personal information. In order to embed this culture of privacy, an organisation needs to make a commitment to treating personal information as a business asset that needs to be managed, secured and respected. Furthermore, emphasis is needed in understanding the importance of protecting personal information for the organisation (OAIC, 2015). Another aspect to examine is the appointment of key roles and responsibilities for privacy management, this includes overall accountability for privacy by a senior staff member. Thus, it is essential to have a staff member responsible for managing internal and external queries, complaints, corrections and access to private information (Ishak, 2015; von Dietze, 2015).

4.2.1.1 Privacy-by-Design

The commitment is to implement a "privacy-by-design" approach. This refers to the adoption of the seven foundational principles of privacy-by-design, in all organisational decisions that include personal information. Cavoukian (2012), refers to these principles as:

- Being proactive, not reactive, but rather be preventative than remedial;
- Consider privacy as the default setting;
- Embed privacy into the design;

- Create full functionality;
- Ensure end-to-end security;
- Create visibility and transparency; and
- Respect a user's privacy.

The organisation needs to distribute resources to support not only the development, but also the implementation of a privacy management plan that aims to align business process with privacy obligations. Therefore, a plan needs to be created to determine how this implementation will be monitored, as well as your goals and objectives for managing privacy (OAIC, 2015). Alongside these plans, reporting mechanisms need to be implemented to ensure that senior management is routinely concerned about privacy issues (Ishak, 2015). The following section examines the second step in the framework.

4.2.2 Step II – Establish

The second step refers to the development and implementation of robust and effective practices, procedures and systems. This section is referred to as the most comprehensive part of the framework, as it refers to segments of the Australian Privacy Principles (APP), which will be discussed in the relevant sections. As such, Step 2 focuses upon several activities that an organisation should focus upon to develop a privacy management framework (von Dietze, 2015). These activities are discussed in the following section, starting with keeping personal information current.

4.2.2.1 Up-to-date Personal Data Inventory

The first activity is the most straightforward activity, as any personal information holdings within an organisation are to be continuously updated. This also includes any off-shore sites, or information in a third party's possession (OAIC, 2015). The next activity focuses upon compliance.

4.2.2.2 Ensuring Compliant Personal Information-Handling Practices

It is important to develop and maintain processes to ensure that during the information lifecycle, all information is handled in accordance with the organisation's privacy obligations. This lifecycle refers to the creation; distribution; use; maintenance and disposition of information (Stephens, 2007). It is imperative to ensure that greater consideration is specified to areas assessed as having greater risk, including the use of external agents, or service providers, contractors, outsourcing arrangements and off-shore storage sites (OAIC, 2015). However, from an internal perspective an

organisation must also consider how staff members are to handle personal information in their everyday duties. It is essential to adapt these processes to align with the different needs of different parts of the organisation, and how they utilise personal information (Ishak, 2015, OAIC, 2015). The following activity concentrates upon privacy awareness.

4.2.2.3 Promoting Privacy Awareness

An organisation needs to integrate privacy into induction and regular staff training programs to promote privacy awareness and obligations throughout the organisation. Furthermore, this should not be limited to permanent staff, but also short term staff, service providers and contractors (OAIC, 2015). The next activity entailed in this step examines privacy policies.

4.2.2.4 Developing Privacy Policies

It is essential that an organisation develops and implements a clearly expressed, up-to-date, privacy policy (OAIC, 2015; von Dietze, 2015). The following is a checklist developed as part of the APP to provide assistance in the development and evaluation of an organisation's privacy policy.

Table 7 - APP privacy policy checklist (OAIC, 2014)

Issue	Yes/No	Comments
Management of Personal Information: • Does the policy explain how personal information is managed?		
Relevance: • Does the policy only include information that is relevant to how you manage personal information?		
Easy to Understand: • Is the policy clearly expressed and understandable?		
Easy to Find: • Is the policy easy to navigate so that people can find information that is relevant to them?		
Specific: • Is the policy tailored to reflect your specific functions, activities and personal information handling practices?		
Tailored: • Is the policy directed at the specific audiences who may be reading it?		
Review: • Has the policy been reviewed recently, to ensure that it reflects your current information handling practices?		

As seen in Table 7, there are several different issues that need to be evaluated first before progressing into the implementation process. The following sectiion examines risk-management.

4.2.2.5 Implementing Risk-Management Processes

Implementing a risk-management processes allows for the identification, assessment and management of privacy risks across all aspects of an organisation, including personal information security risks (Ishak, 2015; OAIC, 2015). Furthermore, strategies such as information security

risk assessments and regular reviews of your personal information security controls need to be integrated into the organisation (OAIC, 2015). The following activity examines another strategy known as a privacy impact assessment.

4.2.2.6 Privacy Impact Assessments

A privacy impact assessment identifies the privacy impacts of a project and describes recommendations for managing, minimising or eliminating any risk impacts (Clarke, 2009). An effective impact assessment is used throughout the development and implementation of a project, using existing project management processes. The OAIC (2015) notes the following steps to follow in ensuring a correct assessment:

- Describe the personal information flows in a proposal;
- Analyse the possible privacy impacts of those flows;
- Assess the impact the project as a whole may have on the privacy of individuals; and
- Explain how those impacts will be eliminated or minimised.

The following subsection discusses the next activity which relates to the processes for privacy enquiries and complaints.

4.2.2.7 Receiving and Responding to Privacy Enquiries and Complaints

An individual who considers that an organisation has breached his/her privacy should complain to that organisation first to allow an adequate opportunity for the complaint to be dealt with by the organisation (OAIC, 2015). Furthermore, where appropriate, the OAIC can make preliminary enquiries into the matter, investigate and/or attempt to resolve the complaint by conciliation. If a complaint is not resolved, or is not finalised on some other basis, the Commissioner may make a determination about whether an interference with privacy has occurred not occurred (OAIC, 2016).

4.2.2.8 Modifying Personal Information

One of the simpler activities, organisational processes, are established to allow individuals to promptly and easily access and correct their personal information when needed (OAIC, 2015).

4.2.2.9 Data Breach Response Plans

Data breaches can be caused by numerous factors, each affecting different types of personal information. These breaches give rise to a range of actual and potential harms to organisations and individuals. Consequently, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved,

and using that risk assessment from previous activities as the basis for determining an appropriate reaction to a breach.

The OAIC (2014) derived the following key points to consider in responding to a breach:

- Contain the breach and do a preliminary assessment;
- Evaluate the risks associated with the breach;
- Perform some form of notification; and
- Prevent future breaches.

Once an organisation has discovered or suspects that a data breach has occurred, it should take immediate steps to limit the breach, and assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach (Madhub, 2004; OAIC, 2014). Furthermore, a part of this step is to determine who needs to be made aware of the breach, both internally and externally at this preliminary stage. Secondly, one needs to determine and evaluate the risks associated with the breach. The following factors need to be considered when assessing the risk, such as the type of personal information involved, and the cause and context of the breach. Thirdly, one needs to also decide upon whether to notify the affected individuals or not, and how this notification is to occur. This notification can be utilised as an essential mitigation strategy that has the potential to benefit both the organisation and the individuals affected by a data breach. While it is an important strategy, it will not always be the appropriate response. Lastly, after steps are taken to mitigate the risks associated with the breach, the organisation needs to thoroughly investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, to develop one (Madhub, 2004; OAIC, 2014). The following section will discuss the next Step in the PMF, evaluation.

4.2.3 Step III – Evaluate

This third step emphasises the importance of systematically examining the effectiveness and appropriateness of privacy practices, procedures and systems to ensure that they remain effective and appropriate. Therefore, in order to fully examine this effectiveness, the OAIC (2015) derived the subsequent aspects that need to be considered:

- Monitor and review – privacy processes are to be regularly monitored and reviewed, this includes assessing the adequacy and currency of practices, procedures and systems, as well as privacy policies and notices;

- Record keeping – documenting compliance with privacy obligations, as well keeping records on privacy process reviews, breaches and complaints.
- Performance measurement – measure performance against privacy management plan, by regularly reviewing the implementation of the framework and the organisations progress towards their objectives and goals; and
- Communication Channels – creating efficient communication pathways between staff and customers, in order to achieve feedback on privacy processes.

Therefore, from the above mentioned it can be noted that the third step highlights the importance of a regular monitoring process. The continuous reviews and assessments of existing privacy practices assist in measuring an organisation's performance against its privacy management plan and seeking feedback from staff and customers on privacy practices (Ishak, 2015; von Dietze, 2015). The following section discusses the fourth and final step in the PMF.

4.2.4 Step IV – Enhance

This fourth step stresses the fact that privacy compliance is an ongoing obligation, and good privacy management requires the organisation to be proactive, forward thinking and to anticipate future challenges (von Dietze, 2015). By continually improving privacy processes, the organisation will ensure that it is responsive to new privacy issues and that implementation will not be a burden (OAIC, 2015). The OAIC (2015) proposes eight action points in response to the evaluation results, which include the following:

- Make changes to practices, procedures and systems by utilising the results of the third step to improve privacy processes;
- Consider using an external agent to identify areas for improvement amongst the privacy processes;
- Adopt a good privacy practice that extends beyond the requirements of the APP;
- Stay informed with issues of development in privacy laws and ever changing legal obligations;
- Continuously monitor and address new security risks and threats;
- Examine and address the privacy implications of new technologies, and implement privacy enhancing technologies to better manage personal information;
- Present initiatives that promote good privacy standards amongst an organisation; and
- Encourage staff to remain privacy aware by engaging them in privacy events.

The following section discusses some cases of privacy breaches that have affected Australia.

4.2.5 Australian Case Studies

The OAIC had noted several studies during their research indicating the impact of negligence towards private patient information, as well as the repercussions that follow if measures are not in place to prevent such privacy breaches.

4.2.5.1 Case Study – Disclosure of Personal Information

A patient was previously a client of a staff member at a health services provider that offered an In Vitro Fertilization (IVF) treatment. The patient received a group email from the staff member, advising of new services that they would be offering. The recipients of this group email had not been blind carbon copied, and so all the recipients had been informed of the patient's email address, which identified her full name, and the fact that she had been a patient of the staff member (OAIC 2015). The staff member acknowledged that the patient's details had been improperly disclosed. However, the matter was resolved by reconciliation, with the staff member agreeing to pay $12,000 in compensation. The health service provider also implemented privacy training for its staff, apologised directly to the patient and offered a further $10,000 worth of medical services, if required in the future (OAIC, 2015). The subsequent subsection 4.1.5.2 examines another example of a data breach.

4.2.5.2 Adobe Systems Software Ireland Ltd

In 2013, Adobe Systems Software Ireland Ltd (Adobe) experienced a cyber-attack that involved the compromise of information relating to at least 38 million Adobe customers globally, including over 1.7 million Australians. The Australian Privacy Commissioner conducted an investigation into the incident, which at the time considered whether Adobe had taken reasonable steps to protect the personal information it held (Purba, 2016). As this breach was recognised as a global incident, the investigation was conducted in co-operation with Data Protection Commissioner of Ireland and the Office of the Privacy Commissioner of Canada (OAIC 2015).

In June 2015, the Privacy Commissioner found that Adobe had failed to take reasonable steps to protect the personal information it held. Furthermore, it was found that Adobe generally took a sophisticated and layered approach to information security and the protection of the organisation's IT systems. However, there was a concern about the manner in which Adobe secured its customers' personal information in the compromised system (OAIC 2015). It was established that these were not protected to the standard required in the circumstances. The financial repercussions of this

data breach were highlighted in a $1 million fine that was handed out to Adobe (Purba, 2016). Following this economic consequence, Adobe took a range of measures to strengthen its privacy framework (OAIC 2015). The following section discusses Hong Kong's perspective on protecting personal information.

4.3 Hong Kong – Privacy Management Programme

Hong Kong's Office of the Privacy Commissioner for Personal Data (PCPD) notes that privacy and data protection cannot be effectively managed if they are merely treated as legal compliance issues. But rather, organisational data users should integrate personal data privacy protection as a part of corporate governance responsibilities. This should be applied throughout the organisation, incorporating business practises, operational process, networked infrastructure as well as physical architectures and service design (PCPD, 2014). Therefore, a privacy management programme serves as a strategic framework to assist an organisation in building a robust privacy infrastructure that is sustained by an on-going review and monitoring process to facilitate compliance (PCPD, 2014; von Dietze, 2015)

Hong Kong's privacy management guidelines are categorised into two main segments, namely Part-A and Part-B. Part-A of the Guide outlines the baseline fundamentals or components of a privacy management programme. Elements such as organisational commitment and programme controls are considered important, while Part-B discusses how to maintain and improve a privacy management programme on an ongoing basis (PCPD, 2014). A privacy management programme should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The components need to be regularly monitored, assessed and updated accordingly to keep a pace with changes both within and outside the organisation. This may encompass changes in such areas as technology, business models, law and best practices (PCPD, 2014). The following section will discuss this segmentation further, beginning with Part-A.

4.3.1 Part-A – Fundamentals of a Privacy Management Programme

Organisations are often advised to appoint someone to oversee the development, implementation and maintenance of the organisation's personal data protection programmes and practices. Policies and processes are always needed, and training of employees is required. For external agents, contracts are required when organisations transfer personal information for processing (PCPD, 2014). This ensures that the information is protected in a manner that is comparable to how the organisation would protect it. Furthermore, organisations require systems in place to respond to data access and correction requests from individuals for their personal information, and

to respond to complaints from employees and customers about the infringement of personal information privacy (PCPD, 2014). The following figure illustrates an overview of Part-A.

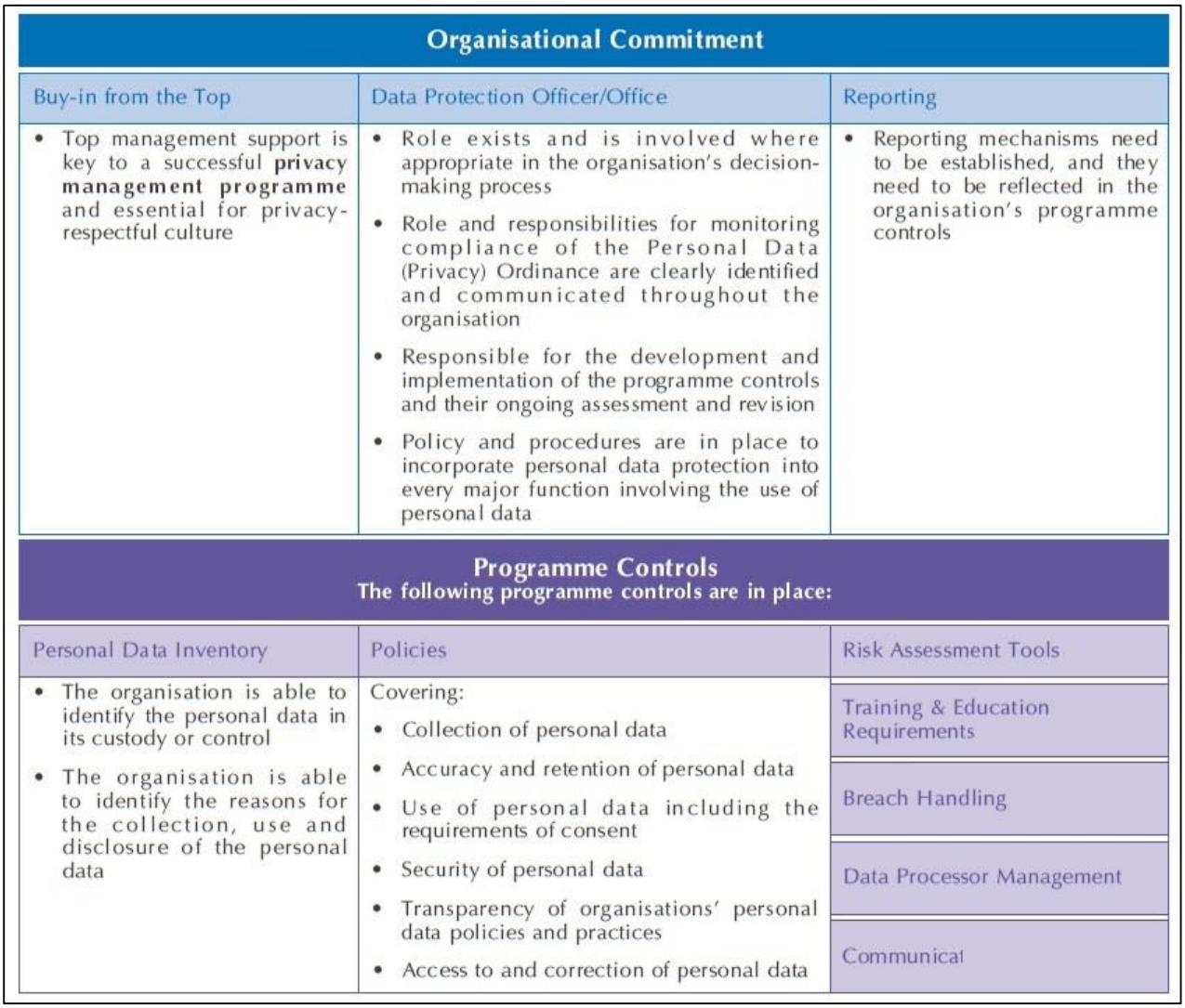


Figure 7 - Part A - Baseline Fundamentals (Privacy Management Programme: A Best Practise Guide. 2014)

4.3.1.1 Organisational Commitment

Organisational commitment is the first component in an internal governance structure that fosters a privacy culture. As such, top management support is an important element for this culture. When top management is committed to ensuring that the organisation is accountable, the privacy programme will have a better chance of success, and a respectful privacy culture will more likely be established (PCPD, 2014; von Dietze, 2015).

4.3.1.1.1 Top Management and Data Protection Officers

Dependent upon the organisational structure, top management or a delegated authority needs to appoint a Data Protection Officer, to endorse the programmes controls as well as to report to the Board. Whether this person is a senior executive of a major corporation or the owner of a small organisation, an individual needs to be assigned the responsibility for overseeing the organisation's compliance with the programme (PCPD, 2014; Yeow & McConnel, 2014). Furthermore, while other individuals may be involved in handling personal information, the Data Protection Officer is usually the one responsible for structuring, designing and managing the programme, including all procedures, training, auditing, documenting, evaluating, and follow-up. Resources need to be directed into training and developing the Officer and his/her team as data privacy professionals (PCPD, 2014; Yeow & McConnel, 2014). Therefore, Data Protection Officers can portray various roles in respect to data protection, but generally their duties are to:

- Establish and implement programme controls;
- Advocate personal information protection within the organisation itself;
- Be responsible for the ongoing assessment and revision of programme controls;
- Co-ordinate with other appropriate persons responsible for related disciplines and functions within the organisation; and
- Represent the organisation in the event of an enquiry relating to an inspection or an investigation by the Privacy Commissioner.

Personal information protection should be seen not just as legal compliance but also in terms of improving processes, customer relationship management, and reputation. The importance of privacy management programme needs to be acknowledged at all levels. It is important to build this into every major function involving the use of personal information, including product development, customer services or marketing (PCPD, 2014). The following subsection examines the expected reporting mechanisms.

4.3.1.1.2 Reporting

Reporting mechanisms need to be established within an organisation to ensure that the right people know how the privacy management programme is structured, as well as whether it is functioning as expected. While within the larger organisations, the audience for this information is expected to be top management, and in turn, top management reports to the board of directors. All reporting mechanisms should be reflected in the organisation's programme controls (PCPD, 2014).

Furthermore, internal auditing and assurances programmes are a prerequisite to monitor compliance standards with personal data protection policies. This could include the form of customer and employee feedback for smaller organisations, or, third-party verifications for larger organisations. Should the organisation be subject to an enquiry, an inspection or an investigation, these reports will assist in demonstrating the organisation's compliance with privacy standards (PCPD, 2014; Yeow & McConnel, 2014). Therefore, an effective reporting programme is able to:

- Clearly define reporting structures as well as employee reporting structures in the event of a complaint or a potential breach;
- Generate tests and reports on the results of its internal reporting structures; and
- Document all reporting structures

The following section discusses the second component of a privacy management programme, the programme controls.

4.3.1.2 Programme Controls

Programme controls assist in ensuring that what is mandated in the governance structure is implemented in the organisation. Developing these controls assists a Data Protection Office to structure an appropriate privacy management programme (PCPD, 2014).

4.3.1.2.1 Personal Data Inventory

An organisation should know what kinds of personal information it holds; how the personal information is being used and whether the organisation really needs this personal information at all. Thus, understanding and documenting the types of personal data that an organisation collects and where it is held is important. This will affect the type of consent the organisation obtains from individuals and how the information is protected. By doing so, it makes it easier to assist individuals in exercising their data access and correction rights (PCPD, 2014; von Dietze, 2015). Every component of an accountable and effective privacy management programme begins with this assessment. Therefore it is essential that an organisation is clear about what kind of personal information it holds and where it is being held. It also needs need to be clear about the reason for the collecting, using and disclosing such information (Yeow & McConnel, 2014). The subsequent section examines organisational policies.

4.3.1.2.2 Policies

Organisations will seek to develop internal policies that give effect to the six data protection principles. These policies should be documented and should show how they connect to the legal

requirements. The PCPD (2014) noted the following key policies that organisations should have in place:

- Collection of personal data;
- Accuracy and retention of personal data;
- Use of personal data including the requirements for consent;
- Security of personal data;
- Transparency of organisations' personal data policies and practices; and
- Access to and correction of personal data.

4.3.1.2.3 Risk Assessment

Often organisations offer services which collect, use or disclose personal data but which have not been thoroughly assessed from a privacy perspective. Through the proper use of risk assessment tools, such problems can be prevented. Furthermore, fixing a personal information privacy problem can be a costly repercussion, so there is careful consideration for a particular initiative, product or service. An assessment that minimises any personal data impacts beforehand is vital (PCPD, 2014). Thus, such assessments should be conducted throughout an organisation, including all projects involving that involve the collection, use or disclosure of personal data. Organisations should develop a process for identifying and mitigating leakage and security risks, which could include the use of privacy impact assessments.

4.3.1.2.4 Training and Education

In order for a privacy management programme to be effective, relevant employees should be made aware of personal data protection generally and to be conversant with the organisations' policies and practices for compliance with the requirements under the programme. Those who handle personal data directly may need additional training specifically tailored to their roles (PCPD, 2014).

Employees will be able to better protect personal data when they are able to distinguish between situations that involve personal data protection. Organisations may have very sound policies and programme controls in place; however, if employees do not commit to these policies the privacy management programme would be made irrelevant (PCPD, 2014). Therefore, employees need to be constantly reminded to comply with the organisation's policies and programme controls until they have become an integral part of their duties. Hence, in order for personal data protection training and education to be effective it should:

- Be conveyed to new employees as an induction programme and periodically thereafter;
- Cover organisational policies and procedures;
- Be delivered in an appropriate and effective manner, based on organisational needs; and
- Circulate essential information to relevant employees as soon as practical if an urgent need arises.

The next section discusses how data breaches are handled.

4.3.1.2.5 Data Breach Handling

Organisations should have a procedure in place and an officer or a designated team responsible for managing a personal data breach. Responsibilities for internal and external reporting of the breach should be clear. While reporting of major data breach to the Commissioner is not mandatory, the Privacy Commissioner encourages organisations to adopt a notification procedure in handling a data breach (PCPD, 2014; Thiel & Kong, 2016). In handling personal data breach, an organisation should consider the circumstances of the breach, and decide whether any of the following persons should be notified as soon as possible:

- Affected data subjects;
- Law enforcement agencies;
- Privacy Commissioner;
- Relevant regulators; and
- Parties capable of taking remedial action to protect personal data privacy.
  (PCPD, 2014)

The following section examines how data processing is managed.

4.3.1.2.6 Data Processor Management

The PCPD (2014) noted various types of obligations that need to be imposed upon a data processor which include the following:

- Security measures to be taken by the data processor;
- Timely return, destruction or deletion of the personal data no longer required;
- Prohibition against other use and disclosure;
- Prohibition against sub-contracting to other service provider;
- Reporting of irregularity;

- Measures to ensure contract staff's compliance with agreed obligations;
- Right to audit and inspect; and
- Consequences for violation of the contract.

The subsequent section discusses the communication aspect of the programme controls.

4.3.1.2.7 Communication

Any communication ought to be clear and easily understandable, as such it should:

- Provide enough information so that the public knows the purpose of the collection, use and disclosure of personal data and how long it is retained;
- Include information on who to contact with questions or concerns; and
- Be made easily available to individuals.

  (PCPD, 2014)

Individuals should be made aware of their ability to access their personal data held by the organisation, and how to request correction or to enquire about the organisation's compliance with the programme (von Dietze, 2015). The next section examines Part-B of the Privacy Management Programme, ongoing assessment and revision.

4.3.2 Part-B – Ongoing Assessment and Revision

As Part-A described the components for creating and establishing a Privacy Management Programme, Part-B provides the outline for the basic tasks involved in the maintenance of the programme, as well as ensuring the ongoing effectiveness, compliance and accountability. However, in order to sufficiently protect personal data whilst meeting legal obligations, the organisation needs to continuously monitor, assess and revise their framework (PCPD, 2014). Table 8 provides an overview of Part B of the program.

Table 8 - Part B - Ongoing Assessment and Revision (adopted from Privacy Management Programme: A Best Practice Guide. 2014)

Oversight & Review Plan	Assess & Revise Programme Controls Where Necessary
Develop an oversight and review plan Data Protection Office or Data Protection Office should develop, oversee and review the plan on a periodic basis that sets out how the effectiveness of the organisation's programme controls will be monitored and assessed,	Update personal data inventory
	Revise policies
	Treat risk assessment tools as evergreen
	Update training and education
	Adapt breach and incident response protocols
	Fine-tune data processor management
	Improve communication

4.3.2.1 Develop an Oversight and Review Plan

As depicted in table 8, the first section of Plan B is to develop an oversight and review plan, which assists the organisation in keeping its privacy management programme on schedule and up-to-date. However, depending on the organisation's compliance standards and control infrastructure, such a plan may be covered in its overall oversight and review system (Yeow & McConnell, 2014; von Dietze, 2015). The plan should establish performance measures and include a schedule of when the policies and other programme controls will be reviewed. The next section discusses assessing and revising programme controls.

4.3.2.2 Assess and Revise Programme Controls

The effectiveness of programme controls should be monitored, periodically evaluated, and revised where necessary. Monitoring is considered to be an ongoing process, and the PCPD (2014) stated that the subsequent questions need to be addressed:

- What are the latest threats and risks?
- Are the programmes controls addressing new threats, and reflecting the latest audit findings?
- Are new services being offered that involve the increased collection, use or disclosure of personal data?
- Is the organisational training necessary and if yes, is it effective?

If any issues are discovered during the monitoring process, concerns need to be documented and addressed by the appropriate individuals. For critical or high-risk processes, internal and external audits are effective methods in evaluating the privacy management programme (Yeow &

McConnell, 2014; PCPD, 2014). Whilst for smaller organisations, checklists should be developed that can be reviewed on a regular basis. However, organisations need to put in place practical measures to ensure that employees or contractors are ensuring organisational policies and procedures.

As mentioned earlier, the privacy management programme is not a universal solution to privacy concerns. Each organisation needs to decide how to structure its own programme by taking into consideration numerous factors which include organisational size; nature of business; as well as the sensitivity and amount of the personal data it controls. Thus it is crucial that assessments of the programme controls discussed under Part A ne conducted in a continuous and thorough manner.

Dependent upon the results of the assessment process, the Data Protection Office mentioned in Part-A needs to consider whether to take action to update and revise the programme controls or not. Therefore in general, a Data Protection Office needs to undertake the following actions:

- Monitor and update the personal data inventory periodically to keep it current;
- Review and revise policies as needed following assessments, audits or responses to breaches;
- Treat privacy impact assessments and security threat and risk assessments as evergreen documents that are continuously modified and evaluated;
- Review and adapt to breach incidents by implementing best practises and recommendations;
- Review and fine tune contracts with external agents; and
- Regularly update and clarify communications explaining data policies and regulations to organisation members and customers.

  (PCPD, 2014)

The subsequent section examines a recent research study to highlight how easily an individual's privacy can be breached, and the importance of a privacy management programme.

4.3.3 Hong Kong Research Study – Misuse of Personal Data

In a research initiative conducted by the Social Science Research Centre of the University of Hong Kong (SSRC), commissioned by the PCPD, a survey was conducted in November and December 2014. The purpose of this research study was to provide the PCPD with knowledgeable

information regarding the public's awareness and perceptions of privacy personal data protection (SSRC, 2014). A sample size of 1 222 respondents were successfully interviewed within Hong Kong. The research indicated that up to 46%, nearly half of the respondents had experienced a breach or misuses of personal information. The most common source of the problem was related to interacting with banks and their systems (57%), followed my telecommunication companies (32%), fitness centres (26%) and money lenders (17%). However, the research goes on to stipulate that those who had not lodged a complaint explained that a friend had provided the information, or they were unwilling to involve the company staff responsible for the privacy breach (SSRC, 2014).

4.3.4 Hong Kong Data Breaches

Thiel and Kong (2016) noted several major data breaches experienced throughout Hong Kong, affecting millions of individuals, including children. The two most significant breaches investigated by the PCPD included:

- SanrioTown – the personal data of up to 3.3 million members of SanrioTown were publicly accessed due to insufficient security protocols; and
- VTech – the inadvertent worldwide disclosure of up to 5 million parents and over 6.6 million related children's profiles.

  (Victor, 2015)

The compromised information contained the names, addresses, gender and birth dates of children, which was a bigger concern to security researchers, as it could allow someone to locate a child's physical address (Victor, 2015). The subsequent section discusses how Sweden and the Organization for Economic Cooperation and Development manages its privacy legislations and policies.

4.4 Sweden and the Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development (OECD) is a unique forum which enables governments to work together to address the economic, social and environmental challenges of globalisation. It is at the forefront of efforts to understand and assist governments in responding to new developments and concerns including corporate governance; the information economy and the challenges of an ageing population (OECD. 2013). The OECD provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies (Kuschewsky, 2014).

One such member of the OECD is Sweden. As with any country, there is a need to develop one's own security protocols to protect its people and their personal information. Sweden is no exception, and has developed the Personal Data Act and Electronics Communications Act. The Personal Data Act aims to protect the privacy of personally identifying information, which it loosely defined as any data that, directly or indirectly, refer to a living entity. Furthermore, users are entitled to information concerning processing of their personal data and, consent must be given before data can be collected. This consent needs to be informed, voluntary, specific, and explicit. While the Electronics Communications Act is mostly concerned with access to the Internet via service providers, it is also concerned with fair use, competition and pricing.

Considering the continuous development and growth of technology and processes, personal data has become ubiquitous and globally accessible. These developments have elevated the risks of an individual's privacy, signalling the need for more effective safeguards (OECD, 2013). The following section discusses the principles which form the OECD Guidelines.

4.4.1 OECD Guidelines

The Guidelines published by the OECD in 1980 were one of the earliest initiatives in the area of data protection, and were the first internationally agreed upon set of privacy principles. The current OECD's basic privacy principles are essentially reflected in all relevant general data protection frameworks worldwide. By following this principles-based approach and being drafted in a technologically neutral manner, the Guidelines have proved to be very flexible and adaptable to technological and societal changes (OECD, 2013; Kuschewsky 2014). There are eight basic privacy principles contained in the Guidelines, as demonstrated in the following table.

Table 9 - Eight Basic Data Protection Principles (adapted from the OECD, 2013)

Guideline	Description
Collection Limitation	Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual
Data Quality	Personal data should be relevant, necessary, accurate, complete and up-to-date.
Purpose Specification	The purposes for the data use should in principle be specified at the time of the collection.
Use Limitation	Personal data should not be used for purposes other than those specified at the time of the collection.
Security Safeguards	Personal data should be protected by reasonable security safeguards.
Openness	Any data collection and processing should be transparent to individuals involved.
Individual Participation	Individuals should have the right to access personal data and have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with the implementing measures.

4.4.2 Reviewing Guidelines

The eight basic privacy principles contained in Table 9 are considered to be comprehensive. Therefore, instead of necessarily changing the Guidelines, the revised Guidelines introduce a number of new concepts. These concepts include privacy management programmes; security breach notification; national privacy strategies; education and awareness as well as global interoperability. The following sections will discuss these concepts further, beginning with privacy management programmes.

4.4.2.1 Privacy Management Programmes

Privacy management programmes play an important role in the responsibility of organisations to protect personal data. Within the revised guidelines, a new section on implementing accountability was introduced. Thus, additional obligations fall upon the data controller, with regard to

establishing a privacy management programme. The essential elements of a privacy management programme include safeguards based upon privacy risk assessment, internal governance structure, oversight mechanisms and incident response plans. The OECD clarifies that such programmes should not only address the controller's own operations, but also cover employees and external agents if necessary. The next section briefly examines breach notifications.

4.4.2.2 Data Security Breach Notification

The onus falls upon data controllers to notify significant parties of security breaches that affect personal data to privacy enforcement or other authorities. Where the breach is likely to adversely affect individuals, the controller should inform these individuals (OECD, 2013). The subsequent sections discusses how data flows.

4.4.2.3 Data Flows

The revised Guidelines indicate that members of the OECD should avoid restricting trans-border data flows amongst themselves; or where the other country substantially observes the Guidelines. But the revised Guidelines places emphasis on the accountability principle, which is explicitly restated in the context of trans-border data flows. However, any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

Additionally, the revised Guidelines recognise the appropriate measures that controllers can implement which, together with effective enforcement mechanisms, can qualify as sufficient safeguards. These safeguards are given fairly moderate flexibility, as they may achieve the required level of protection through various methods. The next section discusses a risk-based approach of the guidelines.

4.4.2.4 Risk-Based Approach

The privacy management programmes should provide for appropriate safeguards based upon privacy risk assessment. The revised Guidelines recognise the importance of risk assessment in the development of policies and safeguards to protect privacy more generally. These changes will be welcomed by organisations as they allow for a certain flexibility and do not impose a generalisation.

4.4.2.5 National Privacy Strategies and Stronger Enforcement

The countries of the OECD were asked to develop national privacy strategies, which needed to be complemented by education and awareness-raising skills; and the promotion of technical measures such as privacy-respecting and privacy-enhancing technologies. Organisations were more likely to face an increased enforcement risk in the future, through joint enforcement action and investigations carried out by supervisory authorities. However, by creating a strong global network of privacy enforcement, authorities were more likely to lead the organisation towards global interoperability.

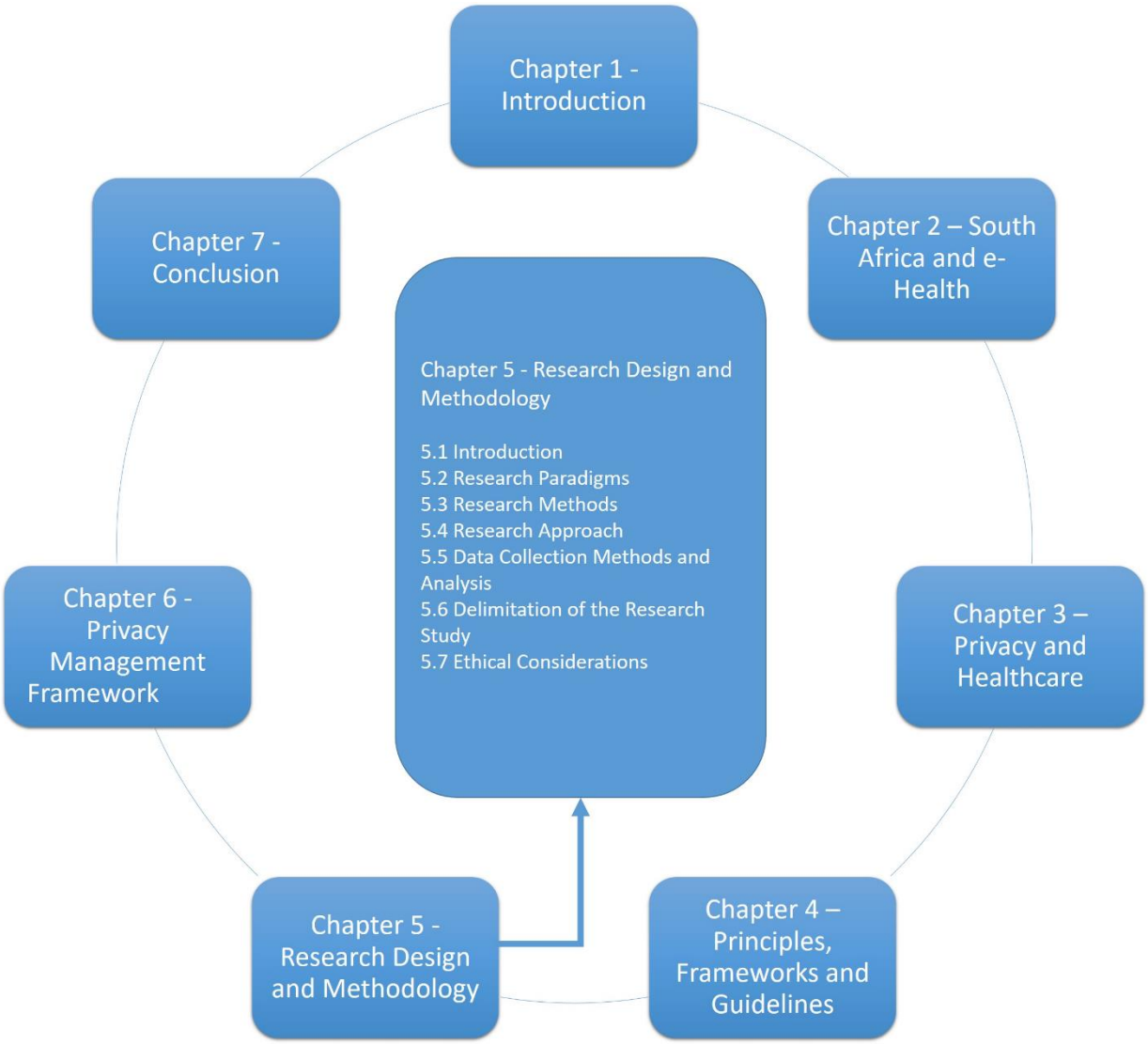
The revised Guidelines explicitly called for the creation of privacy enforcement authorities, which had to be equipped with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis.

In regards to the first tier, the integration of Australia's PMF; Hong Kong's PCPD and the OECD Guidelines, were the most influential factors in developing and refining the PMF alongside the PoPI Act and Conceptual Framework. Within the second tier, the OAIC and PCPD assisted in the progression of document and incident management aspects, while the OECD was more focused upon operations management. However, all three frameworks and guidelines contributed to the development of security management element. Additionally, the PCPD's noted the development of a planning and assessment aspect. Alongside the planning aspect, the OAIC elaborates the need for the monitoring and reporting of the privacy processes. Lastly, in collaboration with the e-Health Strategy guide, the PCPD noted the importance of commitment with managerial support.

4.5 Conclusion

This chapter examined discussed and compared the information privacy standards of three separate countries, Australia, China and Sweden. This refers to Australia's privacy principles and framework Hong Kong's privacy management programme, and Sweden's personal data act and OECD guidelines. From the Office of the Australian Information Commissioner, privacy principles and a framework was developed involved a four step guideline process; embedding a privacy culture; establishing robust and effective privacy processes; evaluating privacy processes and enhancing responses to privacy issues. The guideline offers a list of several commitments that organisations are encouraged to comply with. In comparison, Hong Kong's Office of the Privacy Commissioner for Personal Data derived its own data privacy plan that focused upon organisational data users, and the need to integrate personal data privacy protection as a part of corporate governance responsibilities. This consists of two main parts, the first refers to the appointment of an individual to oversee the development, implementation and maintenance of the organisation's personal data protection programmes and practices. While the second part outlines the basic tasks involved in the maintenance of the programme, as well as ensuring the ongoing effectiveness, compliance and accountability. Sweden developed its own Personal Data Act and Electronics Communications Act, which aims to protect the privacy of personally identifying information. With the support of the Organization for Economic Cooperation and Development forum, several basic data protection principles were integrated into their own privacy act. The following chapter will discuss the research methodology used throughout this research study.

Chapter 5: Research Design and Methodology



5.1 Introduction

The previous chapters served as a basis of the model to be tested in this research study. Chapter two provided a discussion on the impact of PEHRs in South Africa, as well as how the government intends to improve the countries health status. Chapter three was centred upon privacy issues and threats that can affect a patient and healthcare providers or organisations. In addition, Chapter four focused on Privacy Management Frameworks and the role they portray in securing sensitive information. This chapter 5 describes the research designs and methodologies that are applied throughout the study.

A research process is considered to be a scientific method by which information is gathered and analysed. This assists in increasing the understanding of the problem and processes used to find results and accomplish research objectives (Bordens & Abbott, 2002). This chapter is divided into various subsections: these include the research paradigm and the philosophical assumptions; followed by the research methods; data collection and analysis methods in this study. Lastly, the ethical considerations are discussed.

5.2 Research Paradigms

Collis and Hussey (2009) note that from an epistemological perspective, all research must contain a comprehensive foundation within existing knowledge and theory. This ensures that thorough and rigorous research is being performed. As with any study, there is an underlying research paradigm that guides how the research should be conducted (Collis & Hussey, 2009). According to Saunders et al (2007) a research paradigm can be used to study social phenomena from which certain understandings can be achieved. As such, there are various research paradigms which can be used whilst conducting information systems' research. The use of an accepted research paradigm contributes to the integrity of a research study, as it is established upon accepted methods (Olivier, 2009). Oates (2006) acknowledges three philosophical paradigms, these refer to: positivism, interpretivism and critical research. However, Hevner et al (2004) introduced a fourth research paradigm, design science. The following sections will discuss these paradigms further.

5.2.1 Positivist

The positivist paradigm states that reality exists in itself and views the world as independent of human beings, the researchers' beliefs and personal values (Thomas, 2010). Therefore positivist research functions upon two assumptions:

- The world is ordered and regular; and

- The world can be investigated objectively.

Myers (2009) notes that from these assumptions, a positivist's belief is that cause and effect are specific, measurable and independent of the researcher. Furthermore, a positivist viewpoint is considered concrete and fixed. Therefore, reality can be analysed through measurable attributes. The personal beliefs and values of a researcher do not alter the facts observed (Myers, 2009; Thomas, 2010). This assists in ensuring that research can be replicated by different researchers, with the same expected results. The following section examines an interpretivist paradigm.

5.2.2 Interpretivist

In comparison to a positivist paradigm, the interpretivist paradigm is more subjective and dependant on the social context of the researcher. Collis and Hussey (2009) state that researchers therefore rely upon the view and activities of others in reference to how they interpret their own reality. Furthermore, an interpretivist aims to comprehend human behaviour within a specific context, as each individual has his/her own understandings and perceptions of the world (Thomas, 2010). Oates (2006) summarises the characteristics of an interpretivist approach as being:

- Dynamic socially constructed meaning;
- Multiple realities and interpretations; and
- Studying people in their natural setting.

The following sections discuss critical theory and design science.

5.2.3 Critical Theory

Myers (2009) describes critical theory as a focus on the conflicts and contradictions in a social reality, while also relying upon economic, cultural and political influences and history. Therefore critical theory views reality as historically constituted and formed by people (Oates, 2006). Furthermore, critical researchers reject the concept that people need to adapt to technology, but instead argues that society should shape the way technology is created.

In contrast to an interpretivist research, critical researchers acknowledge the impact that their beliefs, values and actions have on their research. However, they criticise interpretive research in failing to analyse the patterns of power and influence that regulate the views of reality (Oates, 2006). The following section will introduce a research paradigm that is becoming increasingly used in the field of IT research.

5.2.4 Design Science

Design science is referred to as a problem-solving paradigm which ensures the creation and application of an artefact. However, in order to create this artefact, design science requires that two activities need to be performed, namely to build and evaluate (Weber, 2010; Peffers et al., 2007). The building process is directed at constructing an artefact for a set purpose, whilst the evaluation process determines how well the artefact performs (Hevner et al., 2004). Figure 8 below illustrates the design science research framework.

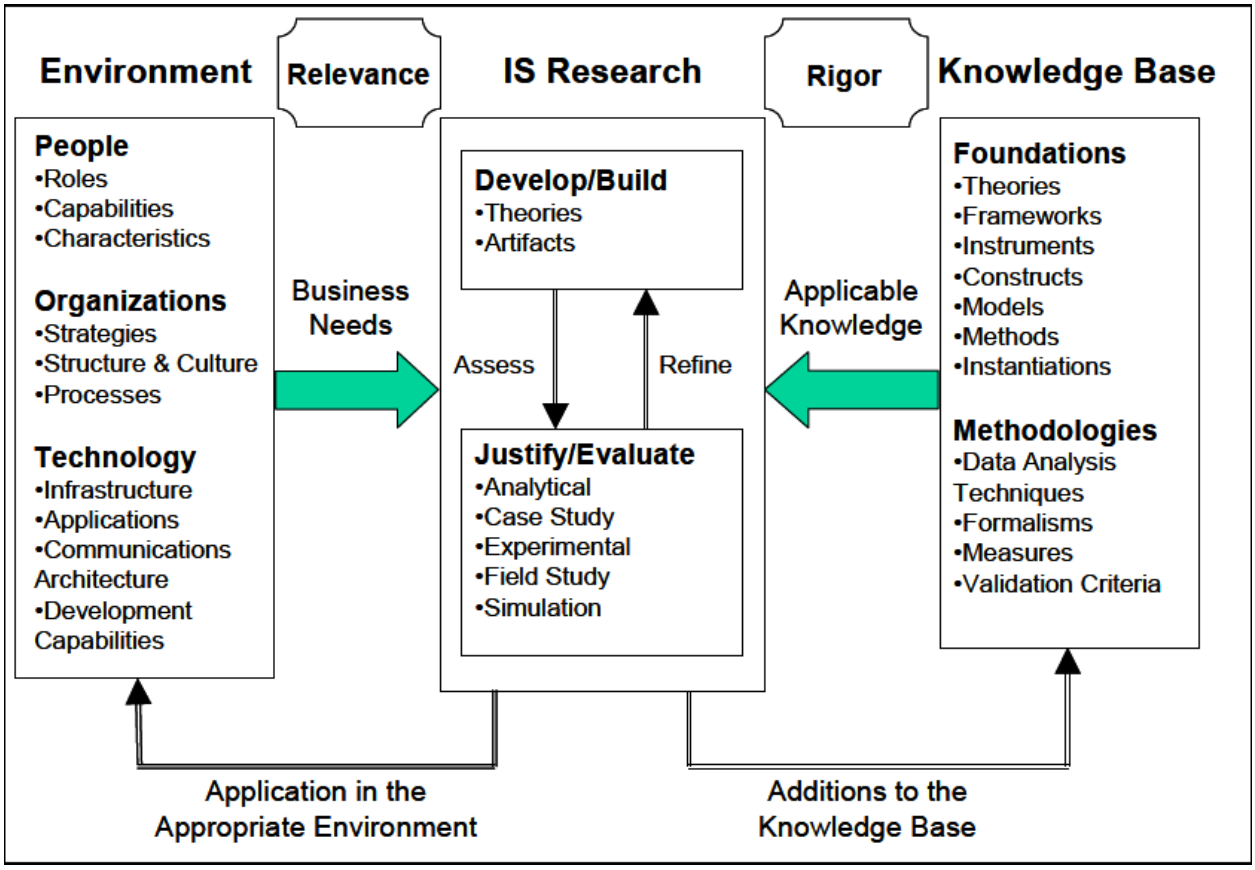


Figure 8 - Information Systems' Research Framework (Hevner et al., 2004)

The design science research framework comprises of three sections: Environment, IS Research and Knowledge Base. The Environment section consists of people, organisations and technology. It ensures that the research problem or opportunity is relevant to the real world. On the other side of the framework is the Knowledge Base. This section ensures rigor in the research, as well as credible and relevant IS research which is used to guide the research study and methodology (Hevner et al., 2004; Vaishnavi & Kuechler, 2015). The final section depicts the IS Research process, illustrating that there are two main phases. These refer to the development of a theory or artefact; and the evaluation or refinement of the theory or artefact (Hevner et al., 2004). The following section provides a philosophical comparison between these paradigms.

5.2.5 Philosophical Assumptions

The philosophical background of a study should not be overlooked, as it affects the way in which the study is conducted. Therefore, the ontological, epistemological and axiological assumptions need to be considered in order to determine an appropriate underlying philosophy of a research study (Collis & Hussey, 2009). Wahyuni (2012) noted the following philosophical assumptions of paradigms which include:

- Ontology – describes the nature of the reality of the world
- Epistemology – explores knowledge; and
- Axiology – focuses on values provided by research.

The following Table provides a comparison of these philosophical assumptions for the research paradigms discussed in section 5.2.

Table 10 - Philosophical assumptions of paradigms (adapted from Collis & Hussey, 2009)

Paradigm	Ontology	Epistemology	Axiology
Positivist	Reality is objectively given and measured using tools or objects independent of the researcher's instruments.	Researcher is independent of what is being researched.	Research is considered value-free and unbiased.
Interpretivism	Reality is socially constructed with multiple realities due to different human experiences.	Researcher interacts with what is being researched.	Research has value and there are biases are present.
Critical Theory	Reality is independent of human thoughts, beliefs and knowledge, but is interpreted though social conditioning.	Researcher interacts with what is being researched, but focuses on explaining the context.	Researcher is biased by world views, cultural experiences and upbringing.
Design Science	Multiple realities	A deeper understanding of information leads to development of an artefact.	Researcher values control over environment and has high tolerance for ambiguity.

From what can be observed in Table 10, a positivist views reality as a concrete structure which is objectively given, while in contrast an interpretivist views reality as a projection of the human imagination. Critical theory considers reality as independent of human thoughts, while design science has multiple, contextually situated realities. The following section will discuss which paradigm was best suited for this research.

5.2.6 Selecting a Paradigm

In comparison to an interpretivist or critical theory, a positivist paradigm is more commonly recognised as the standard for IT research. However, interpretivist research has become more widely adopted in recent years, with design science emerging as the prevailing paradigm in various research areas. Critical theory is not well-known compared to its counterparts, and used less in IT/IS research. In order to determine which paradigm bests suits a research study, Oates (2006) as well as Collis and Hussey (2013) note that selection is dependent upon the nature the research question, personal beliefs and values of the researcher. Therefore, the essential issue is not whether the research should be philosophically informed, but how a researcher is able to reflect philosophical choices and defend them in relation to alternative philosophy. The following figure illustrates where this research study is best situated.

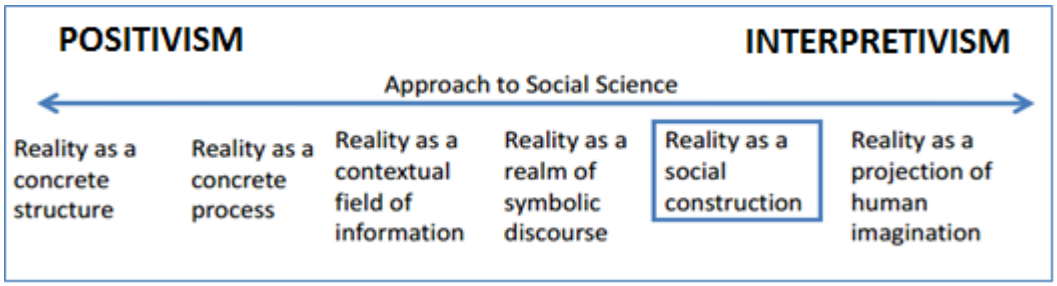


Figure 9 - Continuum of Core Ontological Assumptions (Collis & Hussey, 2013)

The Continuum of Core Ontological Assumptions, illustrated in Figure 9 indicates that this study aligns with the fifth stage of the Continuum: "Reality as a Social Construction". Collis and Hussey (2013) state that "individuals through language, actions and routines create the social world" (p. 49). People are considered to be in a continuous process of interpreting the social world around them; and interpret the actions of others with whom they interact. This interpretation leads to the modification of a person's actions and understanding. Therefore, this research study leans more towards interpretivism rather than a positivist theory, as it seeks to understand the privacy issues that patients might experience whilst using PEHRs on mobile devices. Thus qualitative data was gathered from various journals, articles and case studies in order to identify these concerns. Furthermore, in order to address these issues, a privacy management framework was examined in the previous chapter. This was accomplished by comparing various international policies, strategies and guidelines. The following section will examine the different types of research methods available.

5.3 Research Methods

Collis and Hussey (2009) refer to research methods as the tools used for collecting and analysing data in a research. These methods include qualitative, quantitative and mixed methods. It is imperative that a researcher be able to compare these various methods in order to determine which method is best suited for the research at hand. The following section discusses these methods further, beginning with qualitative.

5.3.1 Qualitative Methods

Qualitative methods are generally used within an interpretivist paradigm, as such used to understand or explain events, human behaviours and causes. The most common methods used in a qualitative research include action research theories, case studies, surveys, in-depth interviews, theories, social interactions, experiences and the Delphi Technique (Goldkuhl, 2012). As qualitative research relates to a naturalistic approach to research, it is concerned with understanding a respondent's attachment to specific phenomena. The researcher analyses the data and relates items of data to other categories. From this, the researcher develops an explanation of events that seek to describe and generalise the cause, reason and process of any social behaviour (Yin, 2015). Therefore, from this description of qualitative research, there are several advantages and disadvantages that need to be discussed.

Atieno (2009) and Anderson (2010) noteda few advantages of qualitative data which include:

- Can complement and refine quantitative data;
- Data collection is usually cost effective;
- Human experience can have a powerful impact on data results, and is often more compelling than quantitative data;
- Research framework can be easily adjusted and its direction altered as new information is received;
- Researchers can examine issues with great detail and depth;
- Researchers can guide interviews, and not be restricted by specific questions;
- The data collected from respondents or cases cannot be generalised to a larger populace, however, findings can be transferred to another setting; and
- The subtleties and complexity about respondents are discovered.

Atieno (2009) and Anderson (2010) also mention various disadvantages of qualitative research that should not be overlooked, these refer to:

- Anonymity and confidentiality possibly creating problems when presenting findings;
- Data analysis that may often be time consuming;
- Difficulty of testing hypotheses and theories;
- Qualitative research sometimes not being well understood and accepted as quantitative research;
- Research quality being dependent upon researcher's skills;
- Research rigor being challenging to assess, maintain and validate;
- Researcher possibly being biased towards opinions;
- Researcher's presence during data gathering possible affecting a respondent's response; and
- The volume of data making analysis and interpretation time consuming.

For this research study, qualitative data was collected and analysed from literature, as well as through the use of expert reviews. The qualitative data which is discussed further in section 5.5. The following section examines the quantitative research method.

5.3.2 Quantitative Methods

Quantitative research is mainly aligned with a positivist paradigm, which focuses on testing a theory and hypothesis. In comparison to qualitative, quantitative methods are more objective and incur statistical and numerical data that can be measured precisely. Therefore, this method encompasses a method that utilises structured data collection, and is usually generated by close-ended questionnaires, surveys and experiments. Researchers generally agree that this research method is often associated with a positivist's paradigm (Bryman & Bell, 2015; Oates, 2006). As such, quantitative data involves questioning respondents in such a structured way, so that the researcher is able to generate facts and statistics to a specific phenomenon (Malhotra, 2012). As with qualitative research, there are advantages and disadvantages that need to be discussed. Bernard and Bernard (2012) as well as Choy (2014) describe the following advantages associated with quantitative research:

- Provides consistent, precise and reliable data;
- Data findings can be generalised if selection process was well designed, and the sample is a true representative of the population;
- Greater objectivity of results, personal bias can be avoided;

- High level of accuracy of results; and
- Relatively easy to analyse findings, but dependent upon volume.

The resulting disadvantages are also noted by Bernard and Bernard (2012), as well as Choy (2014):

- Data may not be robust enough to describe complex issues;
- Difficult to understand context of the study, or is ignored;
- Low response rates;
- More costly compared to qualitative research;
- Research methods may be inflexible, as instruments cannot be modified once research begins; and
- Secondary data is sometimes not available or accessible.

The next section discusses mixed methods as a research method, alongside with its advantages and disadvantages.

5.3.3 Mixed Methods

Mixed methods are known to be the combination of qualitative and quantitative research. It enables the use of any methodological tools required to answer research questions. This is visible in the type of question; the collection of data and the procedures used in data analysis (Oates, 2006). Researchers find mixed methods to be more valid, as it creates further variation in data collection. This in turn, leads to greater validity of research, and allows research questions to be answered from a variety of perspectives (Wiid & Diggines, 2015). Mixed methods also assist in reducing the gaps during data collection, as well as removing any bias throughout the study, by eliminating a researcher's previous assumptions. Therefore, mixed methods research creates a more efficient understanding of the problem statement in comparison to what a single research approach could accomplish (Saunders et al., 2012). Johnson and Onwuegbuzie (2004) describe several advantages and disadvantages to using mixed methods in comparison to using only a qualitative or quantitative approach. They are as follows:

- Combining qualitative and quantitative research produces more complete knowledge to inform theory and practice;
- Mixed methods are capable of adding insights and understanding that might be missed using a single method;
- Mixed methods are capable of providing more effective evidence for a conclusion through the convergence and convergence of findings;

- More inclined to answer a broader and complete range of research questions;
- Pictures, words and narratives can be utilised to add meaning to statistics; and
- Researcher can generate and test a grounded theory.

Alongside the advantages, Johnson and Onwuegbuzie (2004) noted various disadvantages as well that need to be discussed:

- It is considered to be a more expensive and time consuming method;
- Known to be difficult for a single researcher to carry out both a qualitative and quantitative research, especially in conditions where two or more approaches are expected to be used simultaneously;
- Many researchers contend that one should only work with either a qualitative or quantitative research paradigm; and
- Researcher has to be flexible in order to learn multiple methods and approaches in order to mix them efficiently.

Following the identification and classification of research methods for this study, the subsequent section discusses research approaches.

5.4 Research Approach

In conducting research, there are various approaches that can be employed whilst conducting research. Collis and Hussey (2009) classify the most common research approaches as either an inductive or deductive approach. The following sections 5.4.1 and 5.4.2 discuss these approaches respectively.

5.4.1 Inductive Approach

An inductive approach to research refers to theory that is derived from observations of empirical reality to generate general inferences. This form of approach involves moving from theory to hypothesis development and observations, resulting in the validation or disapproval of predicted reality (Collis & Hussey, 2009). Saunders et al (2012) go further and mention that the purpose of an inductive approach is to understand the nature of the problem as well as the context in which the events were taking place. As this approach is best suited for a qualitative research design, it was chosen as the preferred approach for this research study.

5.4.2 Deductive Approach

In comparison to the inductive approach, the deductive approach refers to the study in which a conceptual and theoretical structure is developed and tested through empirical observations. Therefore, particular instances are deduced from general inferences (Saunders et al., 2012). Additionally, the development of approach consists of the development of theories subjected to rigorous testing. As such, the deductive approach is comprised of observation, pattern, tentative hypothesis and, finally, theory. Collis and Hussey (2013) further note that all concepts need to be operationalized in a manner that enables the facts to be quantitatively measured. Table 11 provides a summative comparison between these two forms of research approaches:

Table 11 - Research Approaches (adapted from Saunderset al., 2007)

Approach	Deductive	Inductive
Logic	When premises are true, the conclusion must be true	Known premises are used to generate untested conclusions
Generalizability	General to specific	Specific to general
Theory	Theory falsification or verification	Theory generation and building

The following section will discuss secondary and primary data collection methods and analysis.

5.5 Data Collection Methods and Analysis

Sakhti (2013) refers to data collection as the process by which a researcher gathers information for study purposes in an established and logical manner, as well to answer research questions and assess findings. There are two main sources of data, generally referred to as secondary and primary data (Oates, 2006). For the purpose of this research study, secondary and primary data were collected. The following sections further discusses these types of data collection methods.

5.5.1 Secondary Data Collection methods

Secondary data is referred to as data that has been previously collected by a researcher for a different purpose. As such it already available as a useful guide to the study in question. Secondary data is known to be a time and cost saving method, due to the availability of information and the ease of access to information (Cummings, & Worley, 2014). However, the main disadvantage with secondary data is that it is difficult to explore and source through the vast

amounts of information and the researcher can react subjectively to this information. Additionally, information may be incomplete or outdated, due to drastic changes over time within the environment or technology. This would render secondary data irrelevant to the current situation and mislead the research study (Sakhti, 2013).

For the purpose of this research study, desktop research was utilised as a means of collecting secondary data and, therefore, involved reviewing literature from previous studies. This included articles from academic journals, books in both print and electronic formats, conference proceedings, relevant websites, and theories relating to the study. Various electronic databases were utilised such as ACM Digital Library, Sage Online Journals, Science Direct, Springer Link and Sabinet Reference to find the relevant literature. Furthermore, research study keywords such as 'personal electronic health records', 'information privacy' and 'mobile device' were used as search terms. Case studies of relevant security breaches involving medical records were utilised, as well as current and past integration of PEHR systems. The following section will briefly discuss primary data collection methods.

5.5.2 Primary Data Collection Methods

In comparison with secondary data, primary data refers to data collection whereby an individual collects data from the original source to find solutions to specific research objectives (Wiid & Diggines, 2015). Primary data can be collected by conducting interviews, surveys, observations, experiments, case studies and focus groups (Driscoll, 2011). However, as secondary data collection contains advantages and disadvantages, so does primary data collection. One such advantage is that it enables a greater control over how the information is collected. This fundamentally allows the researcher to determine the number of the respondents, detect problem areas and time frames for completing the data collection process. Furthermore, primary data is collected in relation to specific problems by using procedures that fit the problem best. While secondary data is considered more subjective, primary data is rather objective, thus removing personal bias or misleading information from the field (Collis & Hussey, 2009). However, if the research involves getting feedback from respondents, there is a high probability that the information is biased or inaccurate. Furthermore, designing, preparing and executing questionnaires, surveys, interviews, experiments and observations are often costly and time consuming (Collis & Hussey, 2009).

For the purpose of this research study, five experts from the field of privacy and e-Health were identified in order to evaluate the privacy management framework. The feedback received from

these experts was utilised to refine and adapt the proposed privacy management framework. These experts were identified during the literature review as they had published extensively in the privacy healthcare field, conferences and seminars were also used to identify experts. Subsequently, a research article was accepted, presented and published at the Information Communication and Technology and Society Conference 2017 (Appendix A). Furthermore, these five experts were predominantly contacted via e-mail in order to determine their willingness to participate in this research study, with one round of consultation following on their acceptance to become involved. The following section will discuss how the data would be analysed.

5.5.3 Data Analysis

Data analysis involves interpreting raw data that has been collected during research, and how it will be analysed to the benefit of the study. Therefore, data analysis is the process of determining consistent patterns and summarising relevant details discovered throughout an investigation. Furthermore, all data was streamlined into sensible and logical information (Bryman, 2015; Wiid & Diggines, 2015). Section 5.4 notes the various approaches to conducting research, and as mentioned previously, the information gathered from primary and secondary sources will be analysed in an inductive way. This is to determine whether the observations obtained either support or oppose the theoretical explanation presented in the research. Furthermore, qualitative data will be handled differently, as a thematic analysis of the data will be used and discussed in the following section.

5.5.4 Thematic Analysis

Braun and Clark (2006, p.79) describe thematic analysis as a means of, "identifying, analysing and reporting patterns within data". It is often used within qualitative research, by investigating various themes found within data, and gaining insights and knowledge on the subject. Therefore, thematic analysis assists in organising and describing data in detail (Braun & Clarke, 2006). Furthermore, a thematic analysis is often regarded as a highly inductive process, and a researcher notices patterns or similarities within the data. There are six phases used as guidelines during the analysis process. The following section will discuss these phases further, beginning with data collection.

5.5.4.1 Collecting Data

Data can be gathered from various sources that include transcripts, video and audio recordings, observations, questionnaires, field diaries as well as historical data (Boyatzis, 1998). Once the

data has been gathered, the researcher can move onto the next process, coding and validating the data.

5.5.4.2 Coding and Validating the Data

This phase begins once the researcher has familiarised him/herself with that data, and creates a list of ideas of what is established in the data, and what is interesting about it (Braun & Clarke, 2006). The researcher can then either codify the data by hand or through software applications. Data coding is an explicit and iterative process in which the researcher will modify the analysis, as reflected by data as themes and as ideas emerge (Boyatzis, 1998; Komori, 2011). However, in order to ensure the integrity of codes, more than one researcher should have developed and reviewed the codes. This certifies that the data has not been misinterpreted, and the coding is free of any researcher bias. The data should then be re-read and checked for consistency and validation (Boyatzis, 1998; Braun & Clarke, 2006). Through the integration of codes, a codebook is created from which themes emerge and are identified.

5.5.4.3 Theme Identification

Once all the data has been collected and coded, various themes and patterns emerge from the coded data. Through this process, the focus is shifted to analysing themes at a broader level, and involves sorting the various codes into probable themes, and organising all relevant codes with identified themes. Fundamentally, the researcher analyses his/her codes, and considers how various different code combinations may create a predominant theme (Braun & Clarke, 2006; Komori, 2011).

5.5.4.4 Review Themes

After the various themes have been identified, a further examination and refinement of those themes are required; as such this process involves two levels of reviewing and refining. Initially, the researcher scrutinises all extracts for each theme and determines whether or not a coherent pattern is formed. If a pattern is formed then the researcher can move onto the next level of refining the theme (Braun & Clarke, 2006). This level involves a similar process, but considers the validity of individual themes in relation to the data set, and whether the theme correctly reflects the meanings evident in the data set in its entirety. Therefore, throughout this phase, the researcher re-reads the entire data set for two purposes; the first is to determine whether the themes work in relation to the data set; and the second is to codify any data into additional themes that might have been missed in the earlier phases (Boyatzis, 1998; Braun & Clarke, 2006).

5.5.4.5 Finalise Theme Names

The researcher can finalise the naming and description of themes, by illustrating a few quotations from original text to communicate the intended meaning to the reader (Komori, 2011). As such, it is important that the deception and scope of the content of each theme is as brief and as informative as possible. Otherwise further refinement of the theme is required (Braun & Clarke, 2006).

5.5.4.6 Producing the Report

Once a researcher has a full a description of all the relevant themes, the final analysis and report can be generated. The purpose of the report is to convince the readers of the validity and merit of the researcher's analysis. This can be achieved by analysing each theme and providing data extracts to support the purpose of the research (Braun & Clarke, 2006)

As each expert in the field provides feedback, the information will be broken down, categorised and summarised through thematic analysis. This information will either be utilised to support or oppose the proposed final solution, creating an additional refinement layer for this study. The following section discuss data trustworthiness.

5.5.5 Data Trustworthiness

To ensure that the research data collected has been accurately measured, the validity of the data needs to be determined. According to Mertler (2015), the validity of qualitative data refers to the trustworthiness of this data. For this research study the credibility, dependability and confirmability of the data must be established.

Credibility refers to the results obtained from a qualitative research study being acceptable from the participants' perspective in the research (Mertler, 2015). In order to ensure the credibility of this research, findings will be triangulated. Therefore, information will be collected from various sources, which include expert reviews, legislations as well as academic material in journals' articles, books and questionnaires. Utilising various methods to collect data on the same topic ensures the consistency and validity of the research, as well as determining if the findings support each other. However, Nechkoska (2015) made an important argument by stating that triangulation is not just necessarily a means of cross checking data from numerous sources. It is also a method by which the researcher is able to increase his/her level of knowledge and strengthen his/her standpoint from several perspectives (Nechkoska, 2015).

Dependability emphasises the importance of a researcher being able to account for and describe any changes in the research setting, while noting how these changes affected the way in which the researcher directed the study (Mertler, 2015). A dependability audit can be conducted to confirm the quality and relevance of the study.

Confirmability refers to the ability of the researcher to be able to track the collected data to its source, while the logic that is used to interpret this data should be made explicit (Mertler, 2015). Therefore, in order to accomplish these tasks, the researcher should archive all collected data in a well-organised format that can be made available if the research findings are opposed (Thomas, 2010). The next section discusses the delimitations of this study.

5.6 Delimitation of the Research Study

This research project is focused on the development of a privacy management framework that can be used by healthcare providers to mitigate the privacy concerns of South African patients making use of mobile devices to access PEHRs. This study is focused upon the healthcare sector in South Africa, as well as the issues that correlate with privacy concerns of personal information. Furthermore, this study is mainly concerned with accessing PEHRs with mobile devices and does not focus on EHRs.

5.7 Ethical Considerations

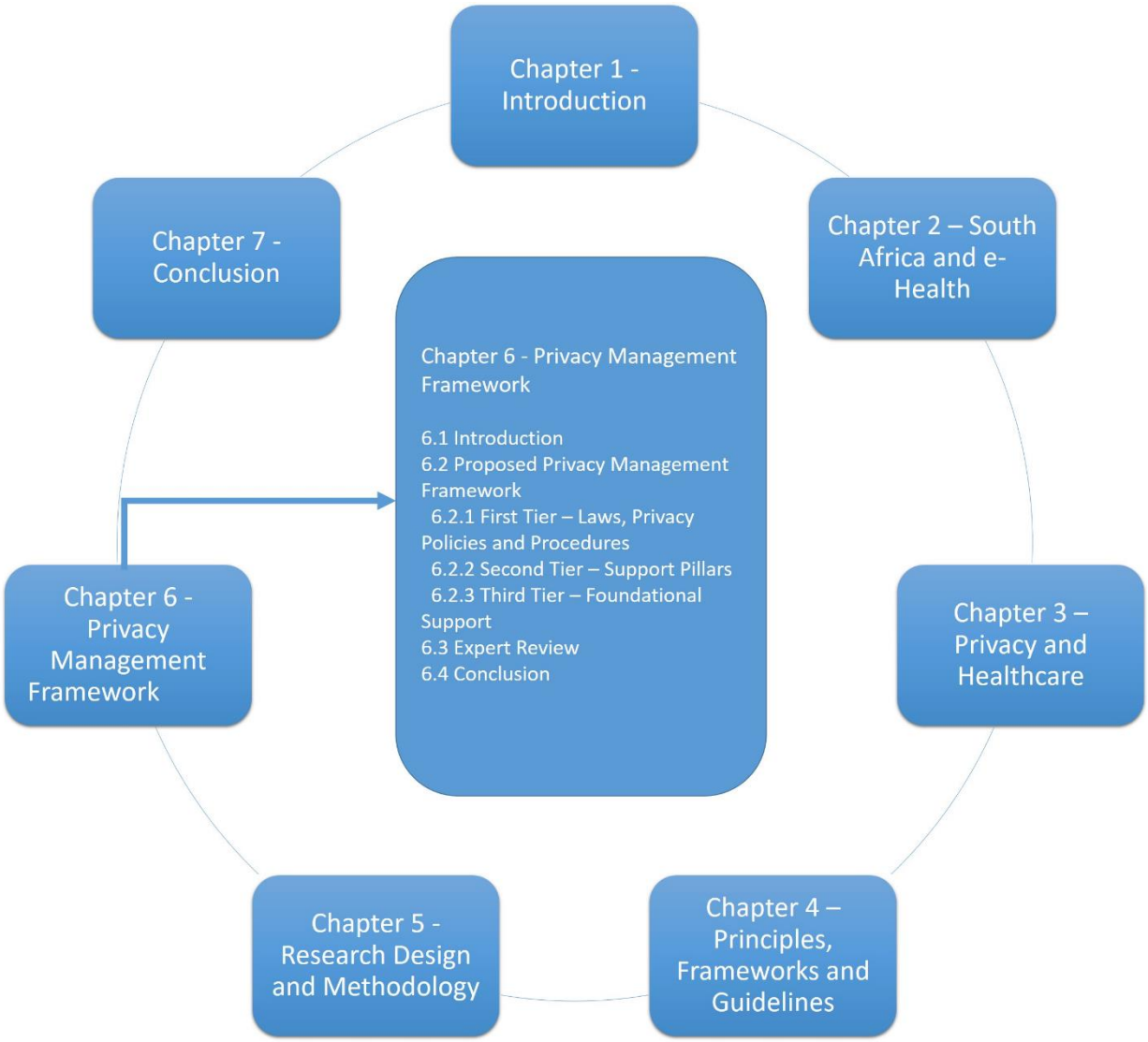
This study is in compliance with the ethical regulations stipulated by the University of Fort Hare's Research Ethics Committee. Therefore, ethical approval was applied for from the University's Research Ethics Committee. Oates (2006) identifies the following rights which will be presented to the participants (experts) during their feedback of this study:

- Wilful participation – the participants (experts) will be encouraged to participate in this research study willingly without any due force;
- Withdrawal – the participants (experts) will be allowed to withdraw from this research study at any time they feel their rights are not considered;
- Informed Consent – prior to the collection of data, the participants (experts) will be informed of how the data will be collected and used, as well as of any third parties that may have access to it; and
- Anonymity – the participants' (experts) identity and location will be withheld unless they provide explicit permission for it to be disclosed.

5.8 Conclusion

This chapter provides an in-depth discussion of the research methodology to be followed by the study. Initially, four research paradigms commonly used in information systems' research were briefly discussed and these assisted in aligning the research study with the appropriate paradigm. Possible research paradigms include a positivist, interpretivist, critical theory and lastly, design science. However, in order to determine which paradigm would best suit the research study, the philosophical assumptions of each paradigm were discussed. This led to the choice of an interpretivist approach to research being selected. Moreover, various research methods were examined and compared, which included qualitative, quantitative and mixed methods. This was followed by a comparison of two common research approaches, inductive and deductive. An inductive approach is the preferred choice for a qualitative research design, and was chosen as the preferred approach for this research study. Furthermore, secondary and primary data collections were discussed. In terms of secondary data collection, desktop research was utilised as a means of gathering information. As for primary data, experts from the field of privacy and e-Health were identified in order to invite them to evaluate the privacy management framework. In order to fully interpret information, data was analysed and themes identified. Finally, the validity, credibility and dependability of data were discussed. The following Chapter will introduce and discuss the proposed privacy management framework.

Chapter 6: Privacy Management Framework



6.1 Introduction

The preceeding chapter discusses the research methodology utilised throughout the research study. This chapter presents the findings of the study, and discusses the proposed privacy management framework (PMF) that could be implemented to assist in ensuring privacy amongst patients that use personal health records through mobile devices. Chapter 3 discusses some of the threats that a patient could encounter through exploitations such as fraud, theft, blackmail as well as discrimination. Although healthcare organisation do have safeguards and controls in place to protect a patients privacy, they are not always guaranteed. Therefore, the integration of compliance and legislation are a necessity for healthcare organisations. This chapter begins by first discussing the proposed PMF, followed by a detailed description of the different categories, characteristics and tiers upon which the framework is built. Finally, the last section discusses the expert review process which was used to further refine the PMF.

6.2 Proposed Privacy Management Framework

A PMF can be considered to be a strategic framework that contains processes and guidelines, capable of assisting an organisation in developing a dynamic and secure privacy infrastructure and culture. For the purpose of this research study, the proposed PMF was constructed by examining both national and international policies, legislations and models which include:

- South Africas National e-Health Strategy Guide and Protection of Personal Information Bill;
- The Conceptual m-Health Framework developed by Avancha, Baxi and Kotz;
- Office of the Australian Information Commissioner's Privacy Management Framework;
- Hong Kong's Office of the Privacy Commissioner for Personal Data's Privacy Management Programme; and
- The Organization for Economic Cooperation and Development Guidelines.

A PMF is able to portray an important role in the responsibility of organisations to protect personal data and ensure privacy of the patient. However, a PMF is an ongoing product that can never be considered to be finished. The different components of the PMF needs to be regularly assessed, evaluated and updated to accomodate changes both within and outside the organisation. This may encompass changes in such areas as technology and policies. Furthermore, the research study indicated that as the rate of mobile device use increased exponentially, so did the privacy risks. Therefore, for the purpose of this study, there needed to be three main tiers from which to derive a suitable PMF to match the privacy concerns of a mobile user for PEHRs in South Africa.

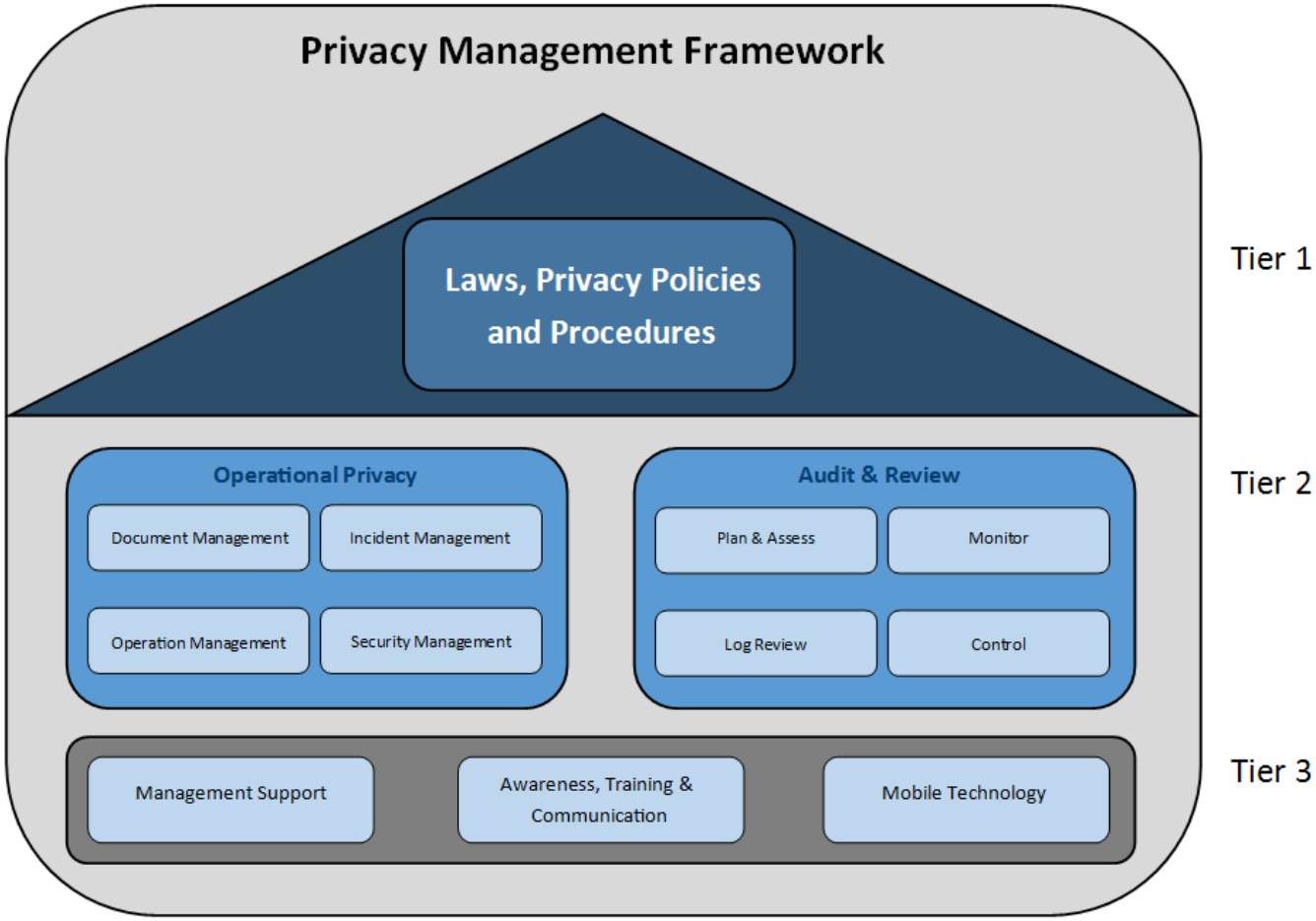


Figure 3 - Proposed Privacy Management Framework

As illustrated in Chapter 1, figure 3, the proposed PMF consists of various partitions which are categorised into three tiers, starting with the first or top tier. The first tier oversees the integration of the PMF through laws, privacy policies and procedures. The second tier is considered to be the two essential pillars of the PMF, and comprises two main components, namely, operational privacy and to audit and review. Both of these pillars consist of various functionalities which will be discussed further in the following sections 6.2.2 and 6.2.3. The third tier serves as the rudimental foundations of the PMF, which deals with awareness and training, communications and support for healthcare organisations and patients. The following section will discuss the tiers of the PMF in further detail, starting with the top tier.

6.2.1 First Tier – Laws, Privacy Policies and Procedures

The first tier relates to organisations' understanding and interpreting of laws, regulations and standards for privacy and data protection, as well as ensuring compliance with those rules. As such, this section examined the current and national information privacy policies, regulations and procedures. This provided a perspective to determine what components and requirements could

be utilised and adapted to enhance information security. It is essential to note that research and development is a continuous activity that seeks to constantly improve life and the environment around us. Therefore, through this tier, the researcher were able to constantly evaluate and monitor policies and regulations, potentially leading to the further development, refinement and adaption of these policies and regulations.

However, an organisation needs to first understand the extent of its geographical reach. If their activities reach international borders, then the privacy laws and regulations of the set country need to be described and integrated into the organisation's current environment. Moreover, the classification of personal information might differ between various counties, therefore without a clear understanding of personal information, it becomes difficult to effectively protect it. Furthermore, privacy policies and legislations are continuously changing and developing, as do advancements towards technology and privacy risks that arise with it. It is important to constantly evaluate and compare present compliances regulations with current ones nationwide, and even international security policies to ensure an up-to-date perspective of protecting privacy. Once an organisation has a successful grasp over current regulatory laws and standards, they are able to create and develop customizable training programmes. This ensures that organisational staff follows correct regulatory privacy procedures and standards.

As mentioned previously within the research, from a South African perspective, the current National e-Health Strategy, and PoPI Act were examined and compared to various international standards. Although not specifically designed for mobile devices and personal health records, aspects of these policies were utilised to assist in creating the conceptual framework. The subsequent section will discuss the next tier of the PMF.

6.2.2 Second Tier – Support Pillars

The second tier relates to the creation of two pillars in an effort to support and sustain the first tier of law, privacy policies and procedures. These two pillars are based upon the elements of operational privacy, as well audit and review. Each pillar contains its own characteristics and aspects, which will be discussed further in the following section, starting with Operational Privacy.

6.2.2.1 First Pillar - Operational Privacy

Operational privacy refers to the integration of a privacy culture into an organisation's operational policies and procedures. This assists in refining and improving privacy processes to ensure that

an organisation is compliant with data privacy regulation and legal requirements. This section contains four constituent parts of the first pillar, starting with document management.

6.2.2.1.1 Document Management

Document management relates to the co-ordination and control of the storage, location, updating and distribution of information in a secure and efficient manner thereby ensuring that they are accessible to authorised personnel when required. Within the PoPI Act, section 3.5.5 notes that a responsible party needs to maintain the documentation of all operations under his/her responsibility. This is supported by Section 4.2.3 under OAIC's PMF evaluation procedure, whereby a similar aspect is mentioned in regard to record keeping. As such, documenting compliance with privacy obligations, as well as keeping records on privacy process reviews, breaches and complaints is vital. The PCPD's privacy programme section 4.3.1.1.2, refers to the creation of a reporting mechanism to define and document reporting structures in the event of a patient complaint or potential information breach. This leads onto the following characteristic, incident management.

6.2.2.1.2 Incident Management

Under section 3.5.8, under the PoPI Act, as well as the OAICs PMF and PCPD privacy program, there is an obligation on the healthcare organisation to respond to privacy breaches promptly. A breach refers to a situation where sensitive and confidential data has been potentially viewed, used or stolen by an external threat (Rouse, 2010). Section 3.3 classified various threats to a patient's private information. These threats refer to the accidental disclosure of information by a patient; data breach by an insider; physical or network based intrusion by an outsider; or simply the curiosity of an insider within the healthcare organisation. Section 6.2.3.3.1 classified these threats in further detail. Research article, Appendix A, stated the consequences of the breach of personal information. These relate to potential liability, negative publicity and the eventual loss of a patients trust in the healthcare provider. Additionally, these threats can affect a patient's safety, privacy as well the confidentiality and integrity of healthcare data. Once the organisation has discovered a breach, it should take immediate steps to limit the breach, and assess whether steps can be taken to mitigate the harm an individual may suffer as a result of it. The following section discusses the third constituent part of the operational privacy pillar, operation management.

6.2.2.1.3 Operation Management

The Conceptual m-Health Framework as well as the PoPI Act put forth several principles that ensure that patients information is collected only for its intended purposes, with explicit consent.

Section 3.5.2 and 3.5.3 describe these principles further, by discussing purpose specification and process limitations. These limitations assist in reducing the unnecessary distribution of PEHRs to external agents, attending doctors or specialists unless required. Additionally, this is supported by section 4.3 under the OECD guidelines, which further stipulate that consent needs to be informed, voluntary, specific, and explicit. The following section examines the final constituent part of the operation privacy pillar, security management.

6.2.2.1.4 Security Management

Security management relates to identification and understanding of organisational assets and as such, is followed by the development and documentation of policies and procedures for protecting a patient's personal information. One such procedure that can be utilised for protecting personal information is risk assessment and analysis. Section 4.2.2.6 under the OAIC's PMF, described guidelines for effective risk assessment, which included describing personal information flows in a proposal; the privacy impacts of those flows; assessing the impact of a project on the privacy of patients, and how these impacts could be mitigated. Section 4.3.1.2.3 under the PCPD's privacy programme noted how fixing a personal information privacy problem can become a costly repercussion for a healthcare organisation. Both the OAIC and PCPD shared a common theme of conducting an assessment throughout an organisation, including all projects that involve personal information.

Healthcare organisations often depend upon security professionals to handle the protection of privacy and data. These can be individuals selected within the organisations, educated and trained to become professionals that ensure compliance activities are carried out across the organisation. Therefore, these professionals become responsible for evaluating the privacy landscape and corresponding legal implications for the organisation. This notion is supported by the PCPD privacy programme, within section 4.3.1.1.1 which indicates the appointment of a Data Protection Officer. The OAIC PMF, section 4.2.1 endorses the selection of a senior officer to regulate programme controls and policies. Additionally, the OECD guidelines further clarify this by stating a controller is required to incorporate safeguards based upon this risk assessment. The following section will discuss the second pillar, audit and review.

6.2.2.1 Second Pillar - Audit and Review

Audit and review focuses upon the development of processes to identify and mitigate personal information breaches. This pillar is based upon four aspects, plan and assess; monitor and report;

log review and control. The following section will discuss these further, starting with plan and assess.

6.2.2.1.1 Plan and Assess

The first aspect discusses how plans need to be established that measure the performance of policies and programme controls, on a periodic basis. The PCPDs privacy program, notes the development of an oversight plan that sets out how the effectiveness of these policies and controlled controls will be monitored and evaluated. The next constituent under the second pillar relates to monitoring and reporting.

6.2.2.1.2 Monitor and Report

Alongside the planning aspect, reporting mechanisms need to be implemented to ensure that the correct people, including senior management, are routinely informed about privacy issues. Additionally, section 4.2.1, the OAIC's PMF, further elaborates that privacy processes are to be regularly monitored and reviewed. This includes assessing the adequacy of practices, procedures and systems, as well as privacy policies and notices. The next constituent discussed is log review and control.

6.2.2.1.3 Log Review

A log review assists in identifying any suspicious activity within the organisation. It is a process that needs to be performed regularly, and in accordance with organisational requirements and standards. The review normally consists of comparing logs against a baseline. A baseline involves determining what events are considered normal for an organisation; the time period for event logs as well as generating reports for event logs. These reports and logs can provide a knowledge base for future investigations (Barreiro, 2011; Cobb, 2011). The following subsection discusses the last constituent, control.

6.2.2.1.4 Control

The last aspect refers to controlling the organisational environment through ethical values, organisational policies and procedures and activities. This creates a form of accountability by ensuring the compliance with the appropriate laws and regulations discussed under section 6.2.1. Furthermore, the control element assists an organisation by improving the efficiency and effectiveness of operations (Council, 2014). The subsequent section discusses the third tier of the PMF.

6.2.3 Third Tier – Foundational Support

As previously mentioned, the third tier is considered to be the foundation upon which the PMF was developed. This tier is concerned with creating privacy awareness amongst a healthcare organisation and patients, by implementing privacy training regimes, setting efficient communication standards and creating ongoing support systems from the top levels of an organisation. Firstly, a discussion on management support.

6.2.3.1 Management Support

The healthcare organisation's commitment and support for the PMF is an important aspect in the creation of a privacy culture. Privacy is an element that needs to be rooted into an organisation's everyday culture. This involves identifying organisational compliance gaps; developing plans to close these disparities; as well as enforcing recommended policies and procedures to do so. Within section 2.5.1 of this research study, the e-Health Strategy Plan notes the essential engagement of stakeholder groups to help manage and mitigate privacy risks. Additionally, Hong Kong's privacy programme further stipulates the importance of this commitment in ensuring a better success rate for the implementation of a PMF. The following section discusses the next aspect of awareness, training and communication.

6.2.3.2 Awareness, Training and Communication

This aspect refers to human resource capital within the healthcare organisation which is able to develop a workforce that is able to innovate, develop, deploy, communicate, manage and secure PEHRs. Section 2.2 noted that South Africa's mobile device ownership had increased dramatically over previous years, creating the perception that digital awareness is constantly on the rise. Therefore, patients are expecting new and innovative services from healthcare organisations. The National e-Health Strategy, under section 2.5 described ICT as an essential instrument for this innovation, however South Africa has a shortage of skilled workers, and the health information system has been described as discontinuous and unorganised. This follows through into the next element of training.

Within section 3.2.1, O'Brien (2010) mentions that benefits of privacy includes the ability of a patient to avoid exploitations such as identify theft, fraud and discrimination. This highlights the importance of protecting personal and private information. South Africa's National e-Health Strategy Guide, discussed in section 2.5, mentions the implementation of training and skill retention strategies to better manage this private information. This is supported by the PoPI Act which ensures that healthcare organisations are able to securely handle private information through

adequate training and education of staff. Chapter 4 mentioned similar actions that were included in the Office of the Australian Information Commissioner's (OAIC) Privacy Management Framework and Hong Kong's Office of the Privacy Commissioner for Personal Data's (PCPD) Privacy Management Programme. These refers to inclusions of privacy awareness programs and obligations throughout the organisation, including external agents. The OAIC focuses upon the need to assimilate privacy into staff training programmes which includes not just permanent staff, but service providers, and external contractors. The PCPD stated that those who handle personal data need further training specifically designed for their roles. Furthermore, section 4.2 notes that organisations are often directed to assign someone to manage the development, implementation and maintenance of the organisation's personal data protection programmes and practices. The following section examines the next element of communication.

Any communication ought to be clear and easily understandable, as discussed in section 4.2.3 within the OAICs PMF, by creating an efficient communication pathways between staff and patient leads to the effective feedback of privacy processes. These processes are also discussed within the Conceptual m-Health Privacy Framework and PoPI Act, whereby it is an organisational obligation to communicate with a patient about any breaches of their privacy. In section 4.2.2.7 under the PCPD's privacy programme, patients need to be informed of the purpose of the collection of their personal information, as well as be able to contact the healthcare organisation with concerns and queries. Additionally, Section 2.9.1, the benefit of PEHRs, from a patient's perspective indicated how PEHRs is able to provide a more complete view of relevant health information for both the patient and healthcare provider. From a different perspective, there is an importance for individuals to be made aware of their ability to access their personal data held by the organisation securely on their mobile device, and how to enquire about the organisation's compliance with the privacy programme. The following aspect discusses mobile technology and the threats entailed.

6.2.3.3 Mobile Technology

Section 2.6.2.2 within Chapter 2 describes mobile devices with computing capabilities and wireless connectivity which can perform as a local data repository to access online PEHRs. These mobile device-based PEHRs are capable of providing real-time access to healthcare data. However, according to the research article, Appendix A, three common security threats relating to mobile devices and use of PEHRs were identified. These refer to an individual with a phone, data in transit, and data at rest.

6.2.3.3.1 Threats to Mobile Technology

The first threat, individual with a phone, can be caused by the misplacement, theft or loss of a mobile device. This could enable unauthorised access to the private information stored on the device. Furthermore, the research article by Els and Cilliers (2017), stipulated that the integrity of the data may be at risk as patients may incorrectly modify their own data. Subsequently, mobile devices often have a limited screen display capacity in comparison to desktops or laptops, therefore relating to a higher inaction cost to access information. Patients may as then need to depend on short-term memory to refer to information no longer visible on the screen. While from a different perspective, patients may intentionally modify their personal information for financial fraud.

The second threat, data in transit, refers to information that is actively moving from one location to another through the networks or storage devices. With this continuous movement of data, it may be vulnerable to sniffing, tapping or message alterations. Individuals may attempt to steal a patient's identify for financial implications.

The last threat relates to data at rest, and refers to data that is not actively moving across networks or devices and is commonly located within a healthcare organisations database. This form of data may be susceptible to malware, hackers or use of file-sharing tools. Furthermore, private information may be released inadvertently by an individual with access to the information for purposes beyond its intentional use.

6.2.3.3.2 Information Security Measures for Mobile Technology

Despite these three privacy threats, the research article further mentions that there are information security safeguards and measures that could be implemented to protect a patient's personal information on a mobile device. Starting with the physical level, onus falls upon the patient for ensuring that passwords and user authentication are enabled on mobile devices. Furthermore, he/she are to maintain physical control by locking and physically securing his/her devices. In the event of discarding, theft or misplacement of a device, the research article recommends the installation and activation of remote wiping for the mobile device.

With regard to data in transit, from an organisational perspective there is a need for data encryption. The moment that data is set in motion, we are unable to completely control it, making it more vulnerable to eavesdropping. Therefore, through data encryption, even if the mobile device is lost or stolen, the data remains confidential and secure. From an individual's perspective, it is the patient's responsibility to ensure the protection of their personal information in public. Patients

need to be made aware of the possible security vulnerabilities in accessing unsecure public Wi-Fi hotspots.

In relation to data at rest, the research article noted importance of data encryption for the protection of personal information within databases, however it is not entirely sufficient. Therefore, there are elements which need to also be considered alongside encryption to ensure no unauthorised access. These elements refer to the use of network and security controls; refuting access to external parties, and managing database keys, certificates and policies. The following section will discuss the evaluation of the PMF through the expert review process.

6.3 Expert Review

As mentioned in the previous chapters, this research study utilised desktop research as means of a collecting secondary data in order develop the PMF, while for primary data collection, experts from the field of privacy and e-Health were identified in order to evaluate this PMF. An expert refers to an individual with comprehensive knowledge, or experience in a certain particular area (Newman, 2014). For the context of this research study, five experts were asked to examine the PMF. A research article based upon this study was presented and published at the Information Communication and Technology and Society Conference 2017 (Appendix A). The comments from the reviewers were also included in this section in order to improve the PMF. These reviews all assisted in creating an additional layer of refinement for the PMF, as well as strengthening its foundations.

There were two main themes that were identified among the comments from the experts. The first related to the need for such a framework to govern the privacy in PEHRs. One of the expert reviewers noted: “Current legislation has too many loopholes as it is not specifically written to address privacy related to PEHRs”. Additionally, the expert mentions that there are no laws in place that adequately address the privacy of patient’s information stored in EHR including PEHRs. The experts believed that the framework could assist with future research towards the development of such laws. Consequently, “The same framework can be applied to all patient information management in health care, be it EHR, mobile health records or any other”.

The second issue dealt with the presentation of the PMF. The PMF in the original state was structured differently. The PMF started at the bottom tier with level 1, and finish at the top the third tier consisting of the laws, privacy policies and procedures that would govern the privacy of the patient making use of a PEHRs. However, one of the experts noted that the direction of the

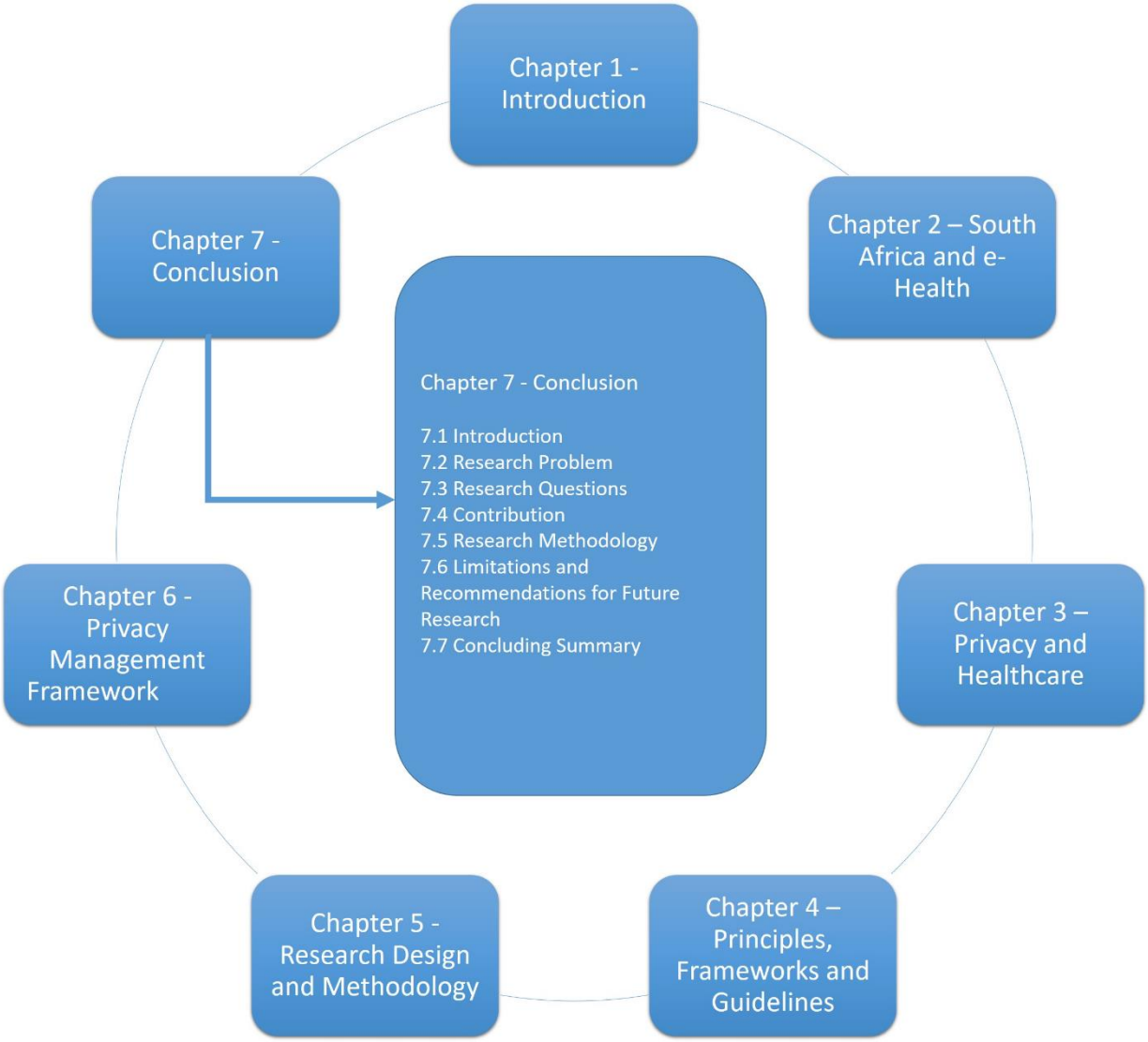
PMF should be reversed, as it created confusion. The expert states, “Organisations will draw reference from the relevant laws and regulations established by the state and the relevant industry oversight”. Comments from other reviewers support the change as their comments refer to the lack of interrelated attributes within the framework, e.g. “How laws and legislation can impact organisational policies?” This comment was addressed by providing more detail in the relevant sections as to how the policies discussed in Chapter 3 will impact on the PMF.

Finally, by taking into consideration the comments expressed by the experts, the structure of the PMF was realigned to better fit an organisational environment, as well as to better describe the impact of laws and legislation on organisational policies and procedures.

6.4 Conclusion

This chapter has presented a proposed privacy management framework for the protection of personal information, aimed at mobile device users. The different categories which form the PMF were discussed; as such there are three different information tiers from which the PMF is derived. Beginning with the top tier, an understanding of an organisations’ interpretation of the law, as well as the impact of rules and regulations for data privacy and protection was established. The next tier discussed the pillars that support the PMF and involves organisational privacy and audit and review operations. The bottom tier consists of three elements that form the foundations of the PMF: which include: management support; awareness, training and communication, and lastly, mobile technology. Within mobile technology, three threats were identified which affects a person’s private information. The last section describe the evaluation of the PMF through an expert review process. The next and final chapter will be a concluding summary of the research.

Chapter 7: Conclusion



7.1 Introduction

This chapter aims to summarise and conclude this research study which was carried out to develop a Privacy Management Framework. The research problem introduced in Chapter 1 will be revisited, followed by the research questions that this research set out to answer, along with a description of how they were answered. This is followed by a summary of the research contribution, methodology and limitations. Finally, suggestions for future research are discussed.

7.2 Research Problem

Through research innovations, mobile-health technologies have identified effective methods to improve the accessibility to health information and services. However, there are also limitations to such health technologies, especially in South Africa, as privacy and security methods are still being developed for mobile technologies. A secured environment is required to protect the privacy of the health information stored in personal electronic health records, including the confidentiality, integrity and availability of this information. From an organisational perspective, there are high costs and negative attributes associated with the breach of patient's privacy and personal information. These threats would affect the patient's trust and confidence in the healthcare organisation. South Africa had introduced the Protection of Personal Information Act, in an attempt to govern privacy concerns. However, the Act was never intended for a mobile health environment, and provides the minimum requirements for processing of personal information. Thus the problem experienced by healthcare providers is the ability to efficiently and effectively protect the privacy of personal electronic health records accessed on mobile devices.

.

7.3 Research Questions

The main research question asks:

How can healthcare providers mitigate privacy concerns of South African patients making use of mobile devices to access personal electronic health records?

In order to answer this research question, the following sub-questions were addressed.

1. How can mobile personal health records improve patient management?

The first sub-questions focused on the effectiveness of mobile health records. Chapter 2 had elaborated on this question by describing the impact of electronic health. This led to the understanding of electronic health records, and more importantly personal electronic health records. The research study indicated that functionality is an essential element of PEHRs, as they are comprised of various components that support healthcare providers and patients in improving the decision-making processes. These functionalities relate to capturing, storing and integrating a

patient's healthcare information. Furthermore, PEHRs were able to reduce medical errors and enhance the monitoring of health conditions. This is achieved through the creation of a central repository that enables an effective communication pathway between patients and healthcare providers. From a healthcare provider's perspective, the quality of healthcare and decision making improves. Furthermore, patients are able to keep a copy of his/her PEHR, reducing the impact of data being lost or damaged.

2. What are the privacy concerns of a South African patient making use of mobile devices to manage their data?

The second sub-question concentrated on the various privacy concerns that patients experienced whilst managing their personal information through mobile devices. Chapter 3 had discussed these privacy concerns by identifying three main threats to patient that use mobile devices PEHRs. The first threat relates to identity, and thereby the misplacement of mobile devices, theft, or unintentional sharing of credentials. The second threat relates to accessing PEHRs. Patient may incorrectly modify their own data, or the design of the device may not user friendly. The last threat refers to the disclosure of the information within PEHRs, which includes both data at rest and in transit.

3. How can a privacy management framework ensure the privacy of South African patients?

The last sub-question focused on how a PMF is able to assist in ensuring the privacy of information in PEHRs. Consequently, in order for PEHRs to assume a fully integrated and success role in healthcare delivery, there needs to be controls in place to ensure patient privacy. Chapter 3 and Chapter 4 had elaborated on these controls further. Within Chapter 3, the discussion of the Conceptual m-Health Privacy Framework provided a basis for mobile health, while the PoPI Act provided a South African perspective to the protection of personal information. The comparison between these two led to the creation of a PMF to support PEHRs. Chapter 4 provided an international perspective and comparison between various privacy frameworks and guidelines. Each chosen country contained different economic, political, and healthcare orientated backgrounds.

With the continuous advancements of technology and processes, personal data is becoming globally available and accessible. This development has increased the risks to an individual's privacy, creating the necessity for more effective and efficient safeguards. In a comparison between the various privacy frameworks and guidelines, there is an indication that privacy and data protection cannot be effectively managed if only treated as a legal compliance. Therefore, a

PMF serves as a strategic framework that assists an organisation in creating a robust privacy infrastructure and controls, in addition to ensuring top-management commitment.

In considering the answers to the above sub-questions has led to the development of a proposed privacy management framework to protect a patients personal electronic healthcare records in South Africa. The framework served as the contribution of this study and will be discussed further in the following section.

7.4 Contribution

The proposed framework was derived from the findings of literature and an expert review. Figure 2 illustrates the iterative process that was followed to develop and refine the PMF. As such, this refinement and development led to the creation of a privacy management framework for South African patients using mobile devices to access PEHRs. In creating a secure privacy framework, patients will be more susceptible to use PEHRs, increasing his/her health standard as well as the South Africa's health status. Figure 3 illustrates the proposed PMF which comprises of three tiers and support pillars.

7.5 Research Methodology

Chapter 5 provides an in-depth description of the manner in which this research study was conducted. The chapter discussed possible research paradigms before justifying interpretivism as the most appropriate paradigm. For this research study, qualitative data was collected and analysed from literature, while the framework was evaluated through the use of expert reviews.

7.6 Limitations and Recommendations for Future Research

The focus of this research study was directed at providing a privacy management framework to address the privacy concerns of personal electronic health records in South Africa. Therefore, the study is focused specifically on PEHRs and not EHRs. Furthermore, as South Africa is considered to be a developing country, future research could include the implementation of the privacy management framework into other developing African countries. This could create a set healthcare privacy standard, and in doing, the overall healthcare standards of developing nations could be improved over time.

7.7 Concluding Summary

This concluding chapter has provided a summary of the research study and the conclusions reached. The research problem is defined and followed by the research questions in order to describe the theoretical background for the study. A summary of how the main research and sub-questions is presented, followed by the contribution made by this research study. The research methodology section briefly discussed how the research study was conducted, alongside the limitations and recommendations for future research.

List of References

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). E-Health cloud: opportunities and challenges. *Future Internet*, 4(3), p.621-645.

Adibi, S. (2015) *Mobile Health: A Technology Road Map*, Bern: Springer

Anderson, C. (2010). Presenting and evaluating qualitative research. *American journal of pharmaceutical education*, 74(8), p.141.

Anonymous., (n.d). *The Hippocratic Oath*. Retrieved June 06, 2016, from Health Professions Council of South Africa: http://www.hpcsa.co.za/hpcsa/default.aspx?id=275

Appari, A., & Johnson, M. E. (2010*).* Information security and privacy in healthcare: current state of research. *International Journal of Internet and enterprise management*, 6(4), p.279-314

Atieno, O. P. (2009). *An analysis of the strengths and limitation of qualitative and quantitative research paradigms*. Problems of Education in the 21st Century, 13(1), p.13-38.

Australian Information Commissioner. (2015). *Privacy management framework: enabling compliance and encouraging good practice*. Retrieved March 08, 2017 from the Office of the Australian Information Commissioner: https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

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

Barreiro, A. (2011). A log Review Process for Detecting Security Incidents. Retrieved March 28, 2017 from TechRepublic: http://www.techrepublic.com/blog/it-security/a-log-review-process-for-detecting-security-incidents/

Basson, B., & Van Zyl, A. (2014). *The right to privacy: how the proposed POPI Bill will impact data security in a Cloud Computing environment*. Stellenbosch: Stellenbosch University, Stellenbosch.

Bernard, H. R., & Bernard, H. R. (2012). *Social research methods: Qualitative and quantitative approaches*. Sage.

Bordens, K. S., & Abbott, B. B. (2002). *Research design and methods: A process approach.* McGraw-Hill.

Botha, A., & Booi, V. (2016). *mHealth Implementation in South Africa*. In IST-Africa 2016 Conference & Exhibition (pp. 1-13). International Information Management Corporation.

Boucher, D. E. (2013). *An Information Privacy Model for Primary Health Care Facilities* (Doctoral dissertation, University of Fort Hare).

Bouri, N., & Ravi, S. (2014). Going Mobile: How Mobile Personal Health Records Can Improve Health Care During Emergencies. *Journal of Medical Internet Research. mHealth and uHealth*, 2(1), e8. http://doi.org/10.2196/mhealth.3017

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Sage.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), p.77-101.

Bryman, A. (2015). *Social research methods*. Oxford University Press.

Calaguas, M. J. (2013). *South African Parliament Enacts Comprehensive Data Protection Law: An Overview of the Protection of Personal Information Bill*. Retrieved March 07, 2016 from https://works.bepress.com/mark_calaguas/15/

Cavoukian, A. (2012). Privacy by design. *IEEE Technology and Society Magazine*, 31(4), p.18-19.

Chase, D. (2011). *Why Google Health Really Failed—It's About The Money*. Retrieved July 28, 2017 from TechCrunch: https://techcrunch.com/2011/06/26/why-google-really-failed-money/

Choy, L. T. (2014). The strengths and weaknesses of research methodology: *Comparison and complimentary between qualitative and quantitative approaches. IOSR Journal of Humanities and Social Science,* 19(4), p.99-104.

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer law & security review,* 25(2), p.123-135.

Cobb, M. (2011). *Best practices for audit, log review for IT security investigations*. Retrieved March 30, 2017 from ComputerWeekly: http://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations

Collis, J., & Hussey, R. (2009*). Business research: A practical guide for undergraduate and postgraduate students*. London: Palgrave Macmillan.

Collis, J., & Hussey, R. (2013). *Business research: A practical guide for undergraduate and postgraduate students*. London: Palgrave MacMillan.

Connelly, R.V. (2011). *What is Personally Identifiable Information* (PII)? Retrieved March 24, 2016 from Render Vision Consulting: http://www.rendervisionsconsulting.com/blog/what-is-personally-identifiable-information-pii/

Council, F. R. (2014). *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*. Retrieved February 20, 2017 from: Financial Reporting Council: https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pd

Cullinan, K. (2013). *South Africa far from targets to reduce maternal, infant mortality.* Retrieved November 23, 2016 from Health e-News: https://www.health-e.org.za/2013/10/29/south-africa-far-targets-reduce-maternal-infant-mortality/

Cummings, T. G., & Worley, C. G. (2014). *Organization development and change*. Cengage learning.

Currie, W. L., & Seddon, J. J. (2014). A cross-national analysis of eHealth in the European Union: Some policy and research directions. *Information & Management, 51(6), p.783-797.*

Dala, P., & Venter, H. (2015). *The extent to which privacy legislation of the European Union and South Africa addresses the 2013 OECD Guidelines*. African Cyber Citizenship Conference (pp. 51-63).

DePoy, E., & Gitlin, L. N. (2015). *Introduction to research: Understanding and applying multiple strategies*. Elsevier Health Sciences.

Dixon, P. (2006). *Medical identity theft: The information crime that can kill you*. Retrieved March 29, 2017 from World Privacy Forum: https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/

Driscoll, D. L. (2011). Introduction to primary research: Observations, surveys, and interviews. *Writing Spaces: Readings on Writing*, 2, p.153-174.

Duffy, J. (2014). *Microsoft HealthVault*. Retrieved August 26, 2017 from PCMag: http://www.pcmag.com/article2/0,2817,2473749,00.asp

e-Health Strategy. (2012). *National e-Health Strategy*. Retrieved August 23, 2016 from the South African National Department of Health: https://www.health-e.org.za/wp-content/uploads/2014/08/South-Africa-eHealth-Strategy-2012-2017.pdf

Els, F., & Cilliers, L. (2017). Improving the information security of personal electronic health records to protect a patient's health information. In Information Communication Technology and Society (ICTAS), p.1-6. IEEE. DOI: 10.1109/ICTAS.2017.7920658

Erasmus, M. (2014). *Perceived Value and Barriers to use of Personal Health Records by Patients in South Africa* (Doctoral dissertation). University of the Witwatersrand.

Esmaeilzadeh, P., Sambasivan, M., & Kumar, N. (2010). *The challenges and issues regarding e-health and health information technology trends in the healthcare sector*. In E-business Technology and Strategy (pp. 23-37). Springer Berlin Heidelberg.

Etzioni, A. (2010). Personal health records: Why good ideas sometimes languish. *Issues in Science and Technology*, 26(4), p.59-66.

Fineberg, A., & Brandt, J. (2014). *Privacy and Security Concerns: Highlights.* Retrieved July 5, 2016 from Healthcare Information and Management Systems Society: http://www.himss.org/privacy-and-security-concerns-highlights

Finn, R. L., Wright, D., & Friedewald, M. (2013). *Seven types of privacy. In European data protection: coming of age* (pp. 3-32). Netherlands, Springer.

Fortuin, J. B., & Naidoo, S. (2015). Opportunities for Teledentistry in South Africa. *South African Dental Journal*, 70(8), p.342-346.

Gaedei, B., & Versteegii, M. (2011). *The state of the right to health in rural South Africa*. South African Health Review 2011, p.99.

Gajanayake, R., Lane, B., Iannella, R., & Sahama, T. (2013). Accountable-ehealth systems: The next step forward for privacy. *Electronic Journal of Health Informatics*, 8(2), p.11.

Garret, P., & Seidman, J. (2014). EMR vs EHR – What is the Difference?. Retrieved September 31, 2016 from HealthIT: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/

Gay, L. R. (1976). *Educational Research: Competencies for Analysis and Application.* Columbus: Merrill.

Gibilisco, S., & Rouse, M. (2013*). Confidentiality, integrity and availability (CIA)*. Retrieved June 15, 2016 from TechTarget: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Givens, B., & Cordary, M. (2012). *California Medical Privacy Fact Sheet C7: Personal Health Records and Privacy*. Retrieved October 14, 2016 from Privacy Rights Clearinghouse: https://www.privacyrights.org/fs/fsC7/CA-medical-personal-health-records#phr%20introduction

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), p.135-146.

Guide to developing an APP privacy policy (OAIC, 2014). Office of the Australian Information Commissioner. Retrieved February 26, 2017 from Office of the Australian Information Commissioner: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-an-app-privacy-policy#steps-in-developing-an-app-privacy-policy

Handling privacy complaints (OAIC, 2016). Office of the Australian Information Commissioner. Retrieved February 26, 2017 from Office of the Australian Information Commissioner: https://www.oaic.gov.au/agencies-and-organisations/guides/handling-privacy-complaints

Hassan, M. A. (2013). *Research Population*. Retrieved August 6, 2016 from Indian Ocean University: http://www.academia.edu/5563491/Research_Population

Healthcare Information and Management Systems Society. (2014). *Electronic Health Records*. Retrieved August 19, 2016 from Healthcare Information and Management Systems Society: http://www.himss.org/library/ehr

HealthVault. (2015). *HealthVault Development Center*. Retrieved June 6, 2016 from Microsoft: https://msdn.microsoft.com/en-us/healthvault/cc196394.aspx

Herman, P. (2016). *75% in Western Cape without medical aid*. Retrieved October 15, 2016 from News24: http://www.news24.com/SouthAfrica/News/75-in-western-cape-without-medical-aid-20160819

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), p.75-105.

HIPAA. (2010). *Health Information Privacy.* Retrieved March 26, 2016 from U.S Department of Health & Human Services: http://www.hhs.gov/hipaa/index.html

Hsu, C. L., Inomata, A., Rahman, S. M. M., Xhafa, F., & Yang, L. T. (2015). *Security, privacy, and applications in mobile healthcare*. https://doi.org/10.1155/2015/675129

Ihonvbere, D. (2010). *Your Business and the CIA Triad: What's your Status?* Retrieved June 28, 2016 from TechPrognosis: http://blog.techprognosis.com/your-business-and-the-cia-triad-whats-your-status/

Ishak, R. (2015). *Privacy Management Framework: the Commissioner's expectations for APP entities*. Retrieved July 04, 2016 from William Roberts: http://www.williamroberts.com.au/News-and-Resources/News/Articles/Privacy-Management-Framework--the-Commissioner-s-expectations-for-APP-entities

Jessup, J., & Neal, E. (2009). *Electronic Transmission of Personally Identifiable Information* Retrieved March 27, 2016 from Office of the Chief Information Officer: http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240

Johnson, M. E. (2009). Data hemorrhages in the health-care sector. *Financial Cryptography and Data Security* (pp. 71-89). Springer Berlin Heidelberg.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 33(7), p.14-26.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014*).* Classification of security threats in information systems. *Procedia Computer Science*, 32, p.489-496. https://doi.org/10.1016/j.procs.2014.05.452

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security: private communication in a public world*. Prentice Hall Press.

Keckley, P.H., & Chung, B. (2010). *The mobile personal health record: technology-enabled self-care*. Washington D.C: Deloitte Center for Health Solutions.

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

Kharrazi, H., Chisholm, R., Van Nasdale, D., & Thompson, B. (2012). Mobile personal health records: an evaluation of features and functionality. *International Journal of Medical Informatics*, 81(9), p.579-593.

Kim, K. & Nahm, E. (2012). Benefits of and barriers to the use of personal health records (PHR) for health management among adults. *Online Journal of Nursing Informatics* (OJNI), 16 (3).

Kingwill, N. (2016). *What is POPI?* Retrieved February 14, 2016 from KPMG: https://home.kpmg.com/za/en/home/insights/2016/05/what-is-popi-.html

Komori, M. (2011). *Thematic Analysis*. March 27, 2016 from Design Research Techniques: http://designresearchtechniques.com/casestudies/thematic-analysis/

Kotz, D. (2011). *A threat taxonomy for mHealth privacy*. In Communication Systems and Networks (COMSNETS), 2011 Third International Conference on (pp. 1-6). IEEE.

Kraan, C. W., Piggott, J. J. H., van der Vegt, F., & Wisse, L. (2015). *Personal Health Records: Solving barriers to enhance adoption.* Retrieved August 30, 2016 from ResearchGate: https://www.researchgate.net/profile/James_Piggott2/publication/280708645_Personal_Health_Records_Solving_barriers_to_enhance_adoption/links/55c1cdce08aed9dff2a4d1d2.pdf

Krist, A.H., & Woolf, S.H. (2011). *A vision for patient-centered health information systems.* Journal of the American Medical Association, 305(3), p.300–301.

Kushchewsky, M. (2014). *Internet of Things Poses a Number of Significant Data Protection Challenges, Say EU Watchdogs*. Retrieved March 29, 2017 from InsidePrivacy: https://www.insideprivacy.com/international/internet-of-things-poses-a-number-of-significant-data-protection-challenges-say-eu-watchdogs/

Kuschewsky, M. (2014). *What does the revision of the OECD Privacy Guidelines mean for businesses?* Retrieved June 17, 2016 from Covington and Burling LLP: https://www.cov.com/~/media/files/corporate/publications/2013/10/what_does_the_revision_of_the_oecd_privacy_guidelines_mean_for_businesses.pdf

Landi., H. (2016). *8.8 Million Patient Records Breached in August*. Retrieved September 09, 2016 from Healthcare Informatics: http://www.healthcare-informatics.com/news-item/cybersecurity/88-million-patient-records-breached-august

Madhub, D. (2004). *Guidelines for Handling Privacy Breaches*. Retrieved May 18, 2016 from Data Protection Office: http://dataprotection.govmu.org/English/Pages/Guidelines/Publications---Guidelines.aspx

Mahajan, A., & Patel, Y. (2012). Enhancing PHR services in cloud computing: patient-centric and fine grained data access using ABE. *International Journal of Computer Science, Information Technology, and Security,* 2(6), p.1130-1135.

Malhotra, N. K. (2012). *Basic marketing research: Integration of social media*. Boston: Pearson.

Maloney, F. L., & Wright, A. (2010). USB-based Personal Health Records: an analysis of features and functionality. *International Journal of Medical Informatics*, 79(2), p.97-111.

Markle Common Framework. (2008). *Common Framework: Overview and Principles*. Retrieved February 07, 2017 from Markle Foundation: https://www.markle.org/sites/default/files/Overview_Professionals.pdf

Masilela, T. C., Foster, R., & Chetty, M. (2013). *The eHealth Strategy for South Africa 2012-2016: how far are we?* South African Health Review, p.15-24.

Matsoso, M. P., & Fryatt, R. (2013). National Health Insurance: the first 18 months. *SAMJ: South African Medical Journal*, 103(3), p.154-155.

Mayo, A. (2012). *Discovery debuts e-health record app*. Retrieved November 16, 2016 from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=55813

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. Retrieved June 19, 2016 from National Institute of Standards & Technology: http://csrc.nist.gov/

McClain, I., & Thompson, E. (2010). The use of cell phone technology provides teens more control and independence and healthcare cost savings in the management of chronic disease. *Perspectives in health information management/AHIMA, American Health Information Management Association*, 7(Fall).

McGee, M. K. (2011). *5 Reasons Why Google Health Failed*. Retrieved July 27, 2016 from Information Week Healthcare: http://www.informationweek.com/healthcare/electronic-health- records/5-reasons-why-google-health-failed/d/d-id/1098623?

Mertler, C. A. (2015). *Introduction to educational research*. London: SAGE Publications.

Monkman, H., & Kushniruk, A. (2013). Considerations for personal health record procurement. Enabling Health and Healthcare Through ICT: *Available, Tailored and Closer*, 183, p.308.

Mosa, A. S. M., Yoo, I., & Sheets, L. (2012). A systematic review of healthcare applications for smartphones. *BMC medical informatics and decision making*, 12(1), p.1. DOI: 10.1186/1472-6947-12-67

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2014). *Personal Health Records: Design considerations for the South African context*. Retrieved August 28, 2016 from Research Space: http://researchspace.csir.co.za/dspace/handle/10204/7712

Myers, M. D. (2009). Qualitative Research in Business & Management. London: Sage Publications.

Narayanan, A,. & Shmatikov, V. (2010). *Privacy & Security – Myths & Fallacies of Personally Identifiable Information*. Retrieved June 17, 2016 from Computer Science Department - The University of Texas: http://www.cs.utexas.edu/

Nass, S. J., Levit, L. A., & Gostin, L. O. (2009). *The Value and Importance of Health Information Privacy.* Retrieved July 27, 2016 from National Institutes of Health: https://www.ncbi.nlm.nih.gov/books/NBK9579/?report=printable

Nechkoska, R. P. (2015). What is triangulation of data in qualitative research? Is it a method of validating the information collected through various methods? Retrieved October 30, 2016 from ResearchGate: https://www.researchgate.net/post/What_is_triangulation_of_data_in_qualitative_research_Is_it_a_method_of_validating_the_information_collected_through_various_methods

O'Brien, C. (2010). *The Importance of Healthcare IT Security*. Retrieved September 25, 2016 from AMAZONAWS: http://blog-static-files.s3.amazonaws.com/uploads/zinnia/Importance+of+Healthcare+IT+Security+-+Charles+O'Brien.pdf

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: Sage Publications.

OECD. (2013). 2013 OECD Privacy Guidelines. Retrieved January 25, 2017 from OECD: https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm to ref

Olivier, M. S. (2009). Information technology research. Pretoria: Van Schaik

ONC National Framework. (2008). *ONC's Office of Interoperability and Standards.* Novmber 20, 2016 from HealthIT: https://www.healthit.gov/sites/default/files/pdf/fact-sheets/onc-office-of-interoperability-and-standards.pdf

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014*).* Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyber Psychology, Behaviour, and Social Networking, 17*(10), p.633-638. DOI: 10.1089/cyber.2013.0585

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, 6(2), p.73.

Patel, V., & Siminerio, E. (2014). *Consumer Access and Use of Online Health Records: It Takes Two to Tango*. Retrieved September 29, 2016 from HealthIT: https://www.healthit.gov/buzz-blog/consumer/consumer-access-online-health-records/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Perrin, C. (2008). *The CIA Triad*. Retrieved October 12, 2016 from TechRepublic: http://www.techrepublic.com/blog/it-security/the-cia-triad/

Pew Research Center. (2015). *Cell Phones in Africa: Communication Lifeline*. Retrieved June 19, 2016 from Pew Research Center: http://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline

Pillay-van Wyk, V., Laubscher, R., Msemburi, W., Dorrington, R. E., Groenewald, P., Vos, T., ... & Somdyala, N. (2014). *Second South African National Burden of Disease Study: Data cleaning, validation and SA NBD List*. Cape Town: Burden of Disease Research Unit, South African Medical Research Council.

Plachkinov, M., Alluhaidan, A., & Chatterjee, S. (2015). *Health Records on the Cloud: A Security Framework.* In International Conference on Health Informatics and Medical Systems (2015) p. 152-158.

Price, M., Bellwood, P., Kitson, N., Davies, I., Weber, J., & Lau, F. (2015). Conditions potentially sensitive to a Personal Health Record (PHR) intervention, a systematic review. *BMC medical informatics and decision making*, *15*(1), p.1.

Privacy Commissioner for Personal Data. (2014). *Privacy Management Programme: A Best Practise Guide*. Retrieved August 27, 2016 from The Office of Privacy Commissioner for Personal Data, Hong Kong: https://www.pcpd.org.hk/pmp/guide.html

Privacy International (2016*). What is Privacy.* Retrieved January 28, 2017 from Privacy International: https://www.privacyinternational.org/node/54

Privacy management framework: enabling compliance and encouraging good practice. (OAIC, 2015). Office of the Australian Information Commissioner. January 30, 2017 from Office of the Australian Information Commissioner: https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

Protection of Personal Information Bill. (2013). Retrieved December 05, 2016 from SAICA: https://www.saica.co.za/TechnicalInformation/LegalandGovernance/Legal/ProtectionofPersonalInformationBill/tabid/2705/language/en-ZA/Default.aspx

Purba, N. (2016). *Adobe fined $1 million for 2013 data breach.* Retrieved June 14, 2017 from WeLiveSecurity: http://www.welivesecurity.com/2016/11/15/adobe-fined-1-million-2013-data-breach/research.

Ross, J., Stevenson, F., Lau, R., & Murray, E. (2015). Exploring the challenges of implementing e-health: a protocol for an update of a systematic review of reviews. *BMJ open*, 5(4), e006773.

Rouse, M. (2010). *Data Breach*. Retrieved June 17, 2017 from TechTarget: http://searchsecurity.techtarget.com/definition/data-breach

SA Health Department. (2015). *White Paper on National Health Insurance*. Retrieved September 02, 2016 from the South African Department of Health: http://www.gov.za/sites/www.gov.za/files/39506_gon1230.pdf

SA Info. (2012). *Health care in South Africa*. Retrieved September 26, 2016 from Brand South Africa: http://www.southafrica.info/about/health/health.htm#.V7wLtlSx-70

SA Justice Department. (2013). *Protection of Personal Information Bill of South Africa*. Retrieved May 18, 2016 from the South African Department of Justice: http://www.justice.gov.za/legislation/acts/2013-004.pdf

Sahu, M., Grover, A., & Joshi, A. (2014). Role of mobile phone technology in health education in Asian and African countries: a systematic review. *International journal of electronic healthcare*, 7(4), p.269-286.

Sakhti, P. (2013). *Methods of Data Collection*. Retrieved May 19, 2016 from SlideShare: http://www.slideshare.net/priyansakthi/methods-of-data-collection-16037781

Salfner, F., Lenk, M., & Malek, M. (2010). A survey of online failure prediction methods. *ACM Computing Surveys*, 42(3), p.1–42. DOI=http://dx.doi.org/10.1145/1670679.1670680

Sarwar, A., & Khan, M. N. (2013). A review of trust aspects in cloud computing security. *International Journal of Cloud Computing and Services Science*, 2(2), p.116.

Saunders, M. L., Lewis, P. & Thornhill, A. (2007). *Research Methods for Business Students*. London: Financial Times Prentice Hall Inc.

Saunders, M. L., Lewis, P. & Thornhill, A. (2009). *Research Methods for Business Students*. London: Financial Times Prentice Hall Inc.

Saunders, M. L., Lewis, P. & Thornhill, A. (2012). *Research Methods for Business Students*. London: Financial Times Prentice Hall Inc.

Schweitzer, E.J. (2012). Reconciliation of the cloud computing model with US federal electronic health record regulations. *Journal of the American Medical Informatics Association, Advance online publication*. doi:10.1136/amiajnl-2011-000162.

Silva, B. M., Rodrigues, J. J., de la Torre Díez, I., López-Coronado, M., & Saleem, K. (2015). Mobile-health: a review of current state in 2015. *Journal of biomedical informatics*, 56, p.265-272.

Sithole, H. L. (2015). An overview of the National Health Insurance and its possible impact on eye healthcare services in South Africa. *African Vision and Eye Health*, 74(1), p.6.

Social Science Research Centre of the University of Hong Kong (SSRC). (2014). *Baseline survey of public attitudes on privacy and data protection*. Retrived August 09, 2016 from Privacy Commissioner for Personal Data: https://www.pcpd.org.hk/english/resources_centre/publications/surveys/surveys.html

Spil, T., & Klein, R. (2014). *Personal Health Records Success: Why Google Health Failed and What Does that Mean for Microsoft HealthVault*?. In 2014 47th Hawaii International Conference on System Sciences (pp. 2818-2827). IEEE.

Srivastava, A., Hossain, M., & Koekemoer, M. (2012). *Legal challenges for M-governance in developing countries: a comparison of India and South Africa*. In *IST-Africa 2012 Conference & Exhibition* (pp. 1-9). International Information Management Corporation.

Steele, R., & Min, K. (2010). HealthPass*: Fine-grained access control to portable personal health records*. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA) (pp. 1012–1019). Perth: IEEE.

Steele, R., Min, K., & Lo, A. (2012). Personal health record architectures: technology infrastructure implications and dependencies. *Journal of the American Society for Information Science and Technology*, *63*(6), p.1079-1091.

Stephens, D. O. (2007). *Records management: making the transition from paper to electronic*. ARMA International.

Sunyaev, A. (2013). Evaluation of Microsoft HealthVault and Google Health personal health records. *Health and Technology*, 3(1), p.3-10. DOI: 10.1007/s12553-013-0049-4

Sunyaev, A., & Chornyi, D. (2012). Supporting chronic disease care quality: design and implementation of a health service and its integration with electronic health records. *Journal of Data and Information Quality* (JDIQ), 3(2), p.3. DOI: 10.1145/2184442.2184443

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine*, *368*(11), p.977-979. DOI: 10.1056/NEJMp1215258

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association, 13*(2), p.121-126. https://doi.org/10.1197/jamia.M2025

Thiel, S., & Kong, A. (2016). *Privacy complaints rise but bigger changes afoot for Hong Kong data privacy.* Retrieved March 20, 2017 from Lexology: http://www.lexology.com/library/detail.aspx?g=c41dd699-ab04-4a62-bed7-0d7d8ebba9e9

Thomas, P. Y. (2010). *CHAPTER 4 Research Methodology and Design*. Retrieved September 10, 2016 from Unisa: http://uir.unisa.ac.za/bitstream/handle/10500/4245/05Chap%204_Research%20methodology%20and%20design.pdf

Thomas, P. Y. (2010*). Towards developing a web-based blended learning environment at the University of Botswana* (Doctoral dissertation). Retrieved January 16, 2017 from UNISA: http://uir.unisa.ac.za/bitstream/handle/10500/4245/03Chap%202_Theoretical%20framework%20and%20literature%20review.pdf?sequence=4

Thomson, L.L. (2013). *Health Care Data Breaches and Information Security: Addressing Threats and Risks to Patient Data.* Retrieved November 16, 2016 from American Bar Association: http://www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.authcheckdam.pdf

Townsend, B. A., & Ncube, C. (2013). *E-health, social media and the law in South Africa can ethical concerns in e-health practice be addressed through regulation*? (Doctoral dissertation). Retrieved August 16, 2016 from University of Cape Town: https://open.uct.ac.za/handle/11427/4741

Tuyikeze, T., & Pottas, D. (2005). *Information Security Management and Regulatory Compliance in the South African Health Sector*. In Information Systems Security Association (pp. 1-12). Retrieved July 20, 2016 from SemanticScholar: https://pdfs.semanticscholar.org/f388/8d19b7585918f08e622f398c56a64b543cbf.pdf

USAid. (2016). *Privacy and Security for mHealth Projects in South Africa*. Retrieved May 18, 2016 from Measure Evaluation: http://www.cpc.unc.edu/measure/resources/publications/fs-15-151

Vaishnavi, V. K., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*. Crc Press.

van Gemert-Pijnen, J. E. W. C., Wynchank, S., Covvey, H. D., & Ossebaard, H. C. (2012). Improving the credibility of electronic health technologies. *Bulletin of the World Health Organization*, 90(5), p.323-323A.

Vance, B., Tomblin, B., Studney, J., & Coustasse, A. (2015). *Benefits and barriers for adoption of personal health records.* Retrieved November 26, 2016 from Marshall Digital Scholar: http://mds.marshall.edu/cgi/viewcontent.cgi?article=1135&context=mgmt_faculty

Victor, D. (2015). *Security Breach at Toy Maker VTech Includes Data on Children*. Retrieved November 01, 2016 from NY Times: https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html?_r=0

van der Westhuizen, E. (2012). *A framework for Personal Health Records in Online Social Networking*. Nelson Mandela Metropolitan University.

von Dietze, A. (2015). *Australian Privacy Management Framework Launched*. Retrieved January 26, 2017 from International Association of Privacy Professionals: https://iapp.org/news/a/australian-privacy-management-framework-launched/

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, 10(1), p.69-80.

Weber, S. (2010). Design Science Research: Paradigm or Approach? *In Association for Information Systems*. p. 214.

Weiss, I. (2016). *EHR vs. EMR.* Retrieved June 8, 2016 from: http://www.practicefusion.com/blog/ehr-vs-emr/

WHO. (2013). *Health Information and Knowledge Management*. Retrieved April 20, 2017 from World Health Organisation Africa: http://www.afro.who.int/en/clusters-a-programmes/ard/african-health-observatory-a-knowledge-management/programme-components/ehealth-and-informatics.html

Wiid, J., & Diggines, C. (2015). *Marketing Research* (3rd ed.). Cape Town: Juta

Wyse, S. (2011). *What is the Difference between Qualitative Research and Quantitative Research?* Retrieved March 16, 2017 from SnapSurveys: http://www.snapsurveys.com/blog/what-is-the- difference-between-qualitative-research-and-quantitative-research/

Xhafa, F., Li, J., Zhao, G., Li, J., Chen, X., & Wong, D. S. (2015*).* Designing cloud-based electronic health record system with attribute-based encryption. *Multimedia Tools and Applications*, 74(10), 3441-3458. DOI: 10.1007/s11042-013-1829-6

Xiao, N., Sharman, R., Rao, H. R., & Upadhyaya, S. (2014*).* Factors influencing online health information search: An empirical analysis of a national cancer-related survey. *Decision Support Systems*, 57, p.417-427. https://doi.org/10.1016/j.dss.2012.10.047

Yeow, M., & McConnel, S. (2014). *Privacy Management Programme: the new regulatory trend in Hong Kong.* Retrieved June 15, 2016 from Clyde and Co: http://www.clydeco.com/insight/article/privacy-management-programme-the-new-regulatory-trend-in-hong-kong

Yerramilli, P. (2015). *South Africa's quadruple burden of disease*. Retrieved April 24, 2016 from PLOS: http://blogs.plos.org/globalhealth/2015/03/southafrica_quadrupleburden/

Yin, R. K. (2014). *Case Study Research Design and Methods* (5th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2015). *Qualitative research from start to finish*. Guilford Publications.