An Information Privacy Model for Primary Health Care Facilities

by

Mr Duane Eric Boucher

An Information Privacy Model for Primary Health Care Facilities

By

Mr Duane Eric Boucher

200804841

Dissertation

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: Prof. Stephen Flowerday

January 2013

ABSTRACT

The revolutionary migration within the health care sector towards the digitisation of medical records for convenience or compliance touches on many concerns with respect to ensuring the security of patient personally identifiable information (PII). Foremost of these is that a patient's right to privacy is not violated. To this end, it is necessary that health care practitioners have a clear understanding of the various constructs of privacy in order to ensure privacy compliance is maintained. This research project focuses on an investigation of privacy from a multidisciplinary philosophical perspective to highlight the constructs of information privacy. These constructs together with a discussion focused on the confidentiality and accessibility of medical records results in the development of an artefact represented in the format of a model. The formulation of the model is accomplished by making use of the Design Science research guidelines for artefact development. Part of the process required that the artefact be refined through the use of an Expert Review Process. This involved an iterative (three phase) process which required (seven) experts from the fields of privacy, information security, and health care to respond to semi-structured questions administered with an interview guide. The data analysis process utilised the ISO/IEC 29100:2011(E) standard on privacy as a means to assign thematic codes to the responses, which were then analysed. The proposed information privacy model was discussed in relation to the compliance requirements of the South African Protection of Personal Information (PoPI) Bill of 2009 and their application in a primary health care facility. The proposed information privacy model provides a holistic view of privacy management that can residually be used to increase awareness associated with the compliance requirements of using patient PII.

DECLARATION

I, **Duane Eric Boucher**, 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 educational institution.

_____

31 January 2013

ACKNOWLEDGEMENTS

They say no man is an island … and it's true that no researcher is either: so many thanks to

- my supervisor – Prof. Stephen Flowerday – for your patience and constructive feedback.
- my work colleagues – Lathelwa, Liezel, Naomi, Ntosh, Roxanne *(a.k.a. the work wife)* and Thayne – for your continued support and encouragement.
- my family – Gran, Mamma, Dad, Jolene, Nicci, Andrew, James, Joshua, Kendra, Liam, and Avery – for being patient with my absence from your lives.
- the members of the Triad – Anne and Ellen – for the magic and mystery you bring to my life.
- my friends – Nolan and Zane – for both spurring me on and asking me if it is actually worth it.
- my friends – Lorna and Lawrence – for showing me that even when life seems dismal, there is always a ray of hope, and that the good person always benefits in the end.
- my feline companions – Squeaks and Smokey – for missing out on many cuddles and tummy scratches.
- the giver of good karma – may I forever find your favour.
- Mom for instilling in me a love of the written word, constantly reproaching me for working way below my potential, and always insisting I work on ten year plans to focus my energy. I have been rudderless over the last five years, but good news; I have a new ten year plan! Finally, Mom, your family misses you deeply, but we know that it was your time to go to Heaven to help share your commitment, courage, love, spirit and strength with any the Lord may deem worthy.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

CCTV	**C**losed **C**ircuit **T**ele**v**ision
CFIP	**C**oncern **F**or **I**nformation **P**rivacy
CPM	**C**ommunication **P**rivacy **M**anagement Theory
EHR	**E**lectronic **H**ealth **R**ecord
EMR	**E**lectronic **M**edical **R**ecord
FIPs	**F**air **I**nformation **P**ractices
NHS	**N**ational **H**ealth **S**ervice
HIPAA	**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
HPCSA	**H**ealth **P**rofessions **C**ouncil of **S**outh **A**frica
INFOSEC	**I**nformation **S**ecurity
ISSA	**I**nformation **S**ecurity **S**outh **A**frica
ISTPA	**I**nternational **S**ecurity, **T**rust and **P**rivacy **A**lliance
OECD	**O**rganisation for **E**conomic **C**o-operation and **D**evelopment
PHI	**P**ersonal **H**ealth **I**nformation
PII	**P**ersonally **I**dentifiable **I**nformation – this includes information that is specific to an individual and can be used to identify them.
POI	**P**rotection **o**f **I**nformation
PoPI	**P**rotection **o**f **P**ersonal **I**nformation *Bill/Act is omnibus privacy legislation for South Africa.*
RALC	**R**estricted **A**ccess/**L**imited **C**ontrol
SAMRC	**S**outh **A**frican **M**edical **R**esearch **C**ouncil

CHAPTER ONE: INTRODUCTION

CHAPTER ONE:
INTRODUCTION

1.1. Background
1.2. Statement of the Problem
1.3. Objectives of the Study
1.4. Research Question
  1.4.1. Secondary Questions
1.5. Significance of the Study
1.6. Literature Review
1.7. Research Methodology
  1.7.1. Data Collection
  1.7.2. Data Analysis
1.8. Delimitation of the Study
1.9. Ethical Considerations
1.10. Outline of the Research Project
1.11. Chapter Summary

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

1.1. Background

The recording of medical information, whether diagnostic or procedural in nature, is not a recent phenomenon, but can be traced to the beginnings of recorded medicine. The Ebers and Smith Papyri, dating from 1600-1550 BCE, and originating in Ancient Egypt, currently provide the oldest known records of medical information (Anon., 2008). It is probably from the knowledge contained in these or similar documents, that Hippocrates learnt to practice medicine, and penned the Hippocratic Oath around 400 BCE. The Hippocratic Oath is significant, because it provides a set of guidelines for the establishment of trustworthy conduct for those practicing the healing arts (Keyser & Dainty, 2005). These ancient guidelines for trustworthy conduct are still being followed. The following phrase taken by health professionals[1] upon obtaining their qualification is the core theme on which this research project is focused, namely:

> "That whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will inviolably secret". Hippocratic Oath (Anon., n.d.)

This means that a health practitioner is required to ensure that the information they possess, either explicit or tacit, about a patient, is kept private, or rather that the patient's privacy rights are honoured. However, health practitioners will at some point during the primary care process find that they need to share information for the benefit of the patient's care with other health practitioners (Agrawal & Johnson, 2007). It is during the process of information sharing that the patient's privacy rights can be compromised when there is a breach in confidentiality, which in and of itself may result in a loss in trust (Petronio & Reierson, 2009; Petronio, 2002). The chance of a data breach occurring increases exponentially as more health practitioners handle the patient's records. Technology further exacerbates the potential for a breach due to

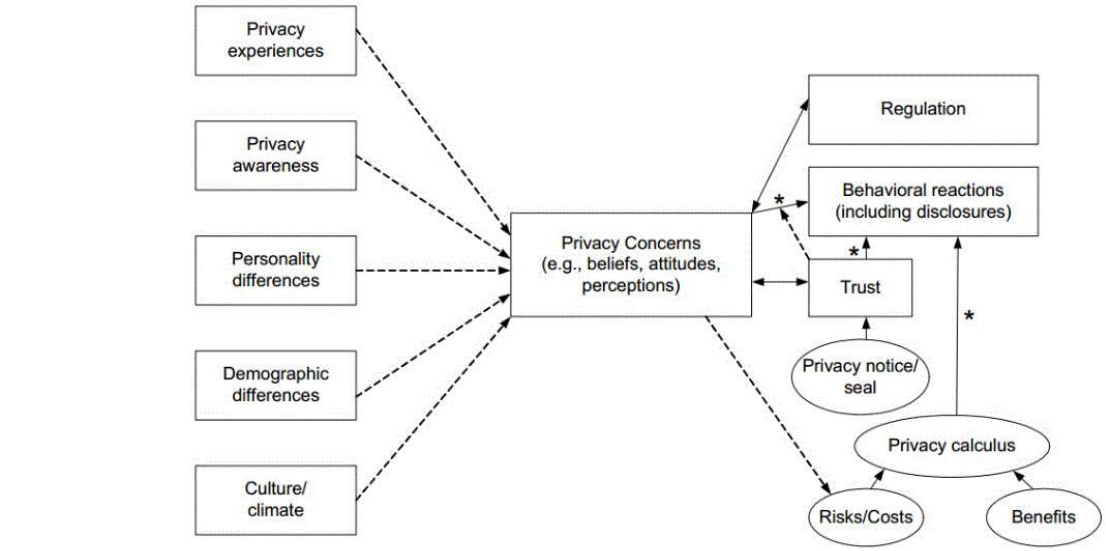
[1] 'Health professionals' are highly skilled workers, in professions that usually require extensive knowledge including university-level study leading to the award of a first degree or higher qualification in a health-related discipline. They are commonly grouped under the general heading of *health practitioners*, which includes those who require formal qualifications, professional body registrations, or unlicensed assistive personnel within the health care sector.

the ease with which electronic health records (EHRs) can be accessed and shared (Angst & Agarwal, 2009). Unfortunately, this makes the safeguarding of privacy all the more complex, as the control of private information becomes more difficult to implement and manage in a technologically progressive environment (Nissenbaum, 2010; Scott, Rundall, Vogt, & Hsu, 2007).

Keeping information private only relies in part on technical mechanisms *(e.g. access control systems)*, but always has its origin in non-technical mechanisms *(e.g. informed consent and contracts of acceptable usage stemming from compliance)* (Narayanan & Shmatikov, 2010). The non-technical mechanisms require individuals to be aware of the decisions that they are making with respect to how their private information will be used in order to reduce the chance of a *privacy paradox* occurring. A privacy paradox occurs when an individual states that they want a high level of privacy, but act carelessly when sharing their private information (Smith, Dinev, & Xu, 2011). In part, it is because they do not necessarily understand how it is to be used by the confidant or a future third party (Smith, et al., 2011). However, 'confidants' don't necessarily treat the information provided with the same care as that person who divulged it in the first place (Petronio, 2002). If private information becomes public, it is impossible to make it private again (Solove, 2008). Often individuals seek legal solutions to solve these problems, but most individuals inadvertently agree to share their private information by accepting a privacy clause in a contract in return for a given benefit (Smith et al., 2011; Nissenbaum, 2010). The benefit the patient wants to realise is effective and efficient health care treatment.

The health care sector is increasingly migrating to the view that the patient is now a health consumer, and must take responsibility for their private information (Angst & Agarwal, 2009). In this regard, the patient is now afforded the opportunity to store their medical information in an online electronic manner, which makes it easier for them to access than the traditional means of visiting the respective health practitioner to either retrieve or update their records. Subsequently, it is imperative that the patient and all the health care stakeholders have an understanding of the different constructs of privacy in order to ensure that it is protected. Smith et al. (2011)

completed an extensive literature analysis of privacy and were able to provide a macro view of privacy (Figure 1.1), which provides a taxonomy of antecedents, privacy concerns, and outcomes. These various constructs will be discussed in this research project, although the focus is more specifically on information privacy in a health care context.



Dotted lines indicate that the relationship is tenuous (i.e., has not been confirmed through repeated studies).

Not shown: Possible two-way loop, in which some actions on the right may impact some constructs on the left.

*Results threatened by privacy paradox, since usually intentions (not behaviors) have been measured.

Figure 1.1: Relationships between privacy and other constructs (Smith et al., 2011, p. 998)

Smith, et al. (2011) state that the physical aspect of privacy is concerned with gaining access to an individual within their private space, whereas information privacy is concerned with accessing an individual's personally identifiable information (PII). How, when, where and why an individual's PII can be accessed raises relevant technical, social and environmental concerns. These concerns can be framed by viewing the context of this research, i.e. the health care sector, as a socio-technical system. The goal of the socio-technical system in health care is to attain operational harmony, so that patient care is both effective and efficient (Whetton, 2005). Although, the technical considerations are important when selecting the correct infrastructure, they are not the focus of this research. Nissenbaum (2010) states that the problems arising with most technical systems can be traced back to a lack of understanding of how social interactions influence their use, especially with respect to information privacy.

This research project will therefore focus on the non-technical (social) aspects of privacy, confidentiality and accessibility when explaining information privacy. Naturally, from time to time during the discussion reference will be made to how individuals use technical systems.

The chapter discussion to follow is an overview of the research project. It provides the research question being investigated and summarises the literature covered in this research project. To frame the literature discussion four theories are introduced. Thereafter, the research methodology applied during the research process in order to realise the objective of this research project is detailed, namely: the development of ***an information privacy model*** to assist in improving the information security awareness of privacy compliance requirements at primary health care facilities.

1.2. Statement of the Problem

The implementation of an electronic medical record (EMR) system in a primary health care facility[2] might be assumed to be plug-and-play, because all medical care follows fundamentally the same procedures; however, this is far from reality (Heeks, 2006). Disparities in technology and more specifically processes may differ from one primary health care setting to the next (Appari & Johnson, 2010; Tjora & Scambler, 2008). Nevertheless, common themes such as concerns of privacy and confidentiality emerge in health care literature with the digitisation of medical records (Smith, et al., 2011; Angst & Agarwal, 2009; Dunnill & Barham, 2007).

The main concern is that patients and the health care practitioners have different perceptions and understandings of their actions with respect to privacy rights (Appari & Johnson, 2010). They also have limited understanding of the various information privacy constructs contained in legislation, regulations, and standards that assist in detailing how PII can be effectively and efficiently managed (Appari & Johnson, 2010).

[2] A *primary health care facility* in this research project refers to any point of first contact between the patient and a health care practitioner, such as: a doctor's practice; a medical clinic; a hospital, where a medical record is created, read, or updated.

This limited understanding of privacy compliance issues is considered a problem which threatens the privacy, confidentiality, and accessibility of EMRs for the treatment of patients and the efficient operations of primary health care facilities.

1.3. Objectives of the Study

The primary objective of this study was to develop an information privacy model for primary health care facilities. Its residual purpose is to aid in improving information security awareness of compliance issues amongst stakeholders within a health context with respect to how, when, where and why EMRs are accessed.

1.4. Research Question

How can the awareness of concerns surrounding privacy and confidentiality influence the accessibility to electronic medical records[3] at a primary health care facility?

1.4.1. Secondary Questions

In order to realise the primary objective it is necessary to answer the main research question, which was done by addressing three secondary questions.

Q1: What are the constructs and legal implications of information privacy?

A multi-disciplinary literature investigation into the concept of privacy is conducted by reviewing the philosophical foundations of privacy, the arising legislation, and the standards that are associated with detailing how to comply when managing PII. Reference is made throughout the investigation to how privacy impacts on a patient's perceived and actual ownership of their information, and how they can restrict access thereto.

[3] An *electronic medical record* (EMR) allows for patient data to be entered directly into the computer and integrates data from various types of medical data into the medical record. There is also increased sharing of information between facilities with multi-EMRs (Whetton, 2005).

Q2: What confidentiality considerations exist with respect to the patient-health care practitioner interaction?

The dynamics of the patient-health care practitioner relationship is investigated by completing a multi-disciplinary literature review of the concepts of confidentiality, trust, and the significance of controls. The information presented assists in providing insights into what influences the patient's acceptance of the sharing of their private information within a collective privacy boundary, and details the level of control they have when sharing information with others.

Q3: What factors affect the accessibility of electronic medical records in a primary health care facility?

The concerns (i.e. associated with information - collection, errors, unauthorised access, and secondary use) with respect to the privacy and confidentiality associated with the accessibility of EMRs are investigated. The discussion is focused on the social aspects attributed to how individuals can restrict access through consent and how various remedies attempt to protect PII where control is limited. The various alternatives to minimise the concerns, including establishing an information security culture focused on information privacy awareness, are discussed.

1.5. Significance of the Study

People (patients and health care practitioners) are an important layer of security within the primary health care facility (Agrawal & Johnson, 2007). They need to assist in ensuring that private information is not accessed or utilised in an unauthorised manner (Appari & Johnson, 2010). This can only be accomplished by making the individuals concerned aware of the threat that they can pose to the private information within their control (Grandison & Bhatti, 2010). The incidence of data breaches are increasingly at risk of occurring, as individuals are amongst the top threats to information assets (Ciampa, 2010; Whitman & Mattord, 2009; Grams & Moyer, 1997). It is therefore increasingly necessary that arising threats and risks to information privacy be reduced in order to avoid litigation from failed compliance with the relevant legislation, regulations, and standards. This can only occur if health care

practitioners and health care workers in general become knowledgeable and responsive to the impact of compliance requirements with respect to privacy and confidentiality on their day-to-day activities (Appari & Johnson, 2010; Deshefy-Longhi, Dixon, Olsen, & Grey, 2004).

1.6. Literature Review

The focus of the literature for this study is in the field of health informatics. Health informatics is the convergent point of information science, health care, and information technology (Whetton, 2005), or information systems and health care. The increasing significance of the EMRs for patients is being driven by the need to improve the management and profitability of the health care sector through increased compliance (Grandison & Bhatti, 2010). The focus in popular media is on the EHR, that moves the need for compliance from the health provider to the patient, or health consumer (Angst & Agarwal, 2009). However, the reality is that EMRs are a more significant portion of the type of patient records in use (Appari & Johnson, 2010; Angst & Agarwal, 2009). EHRs also rely on technologies that may not be available to all, e.g. Internet access. **The focus of this study is therefore on the electronic medical record (EMR), which is typically located at a primary health care facility, and is accessible by the patient through their interaction with the health care workers at the facility**. A primary health care facility is typically a location that is a first point of contact between the patient and their treatment needs, e.g. a clinic, or hospital. The sizes of these facilities vary dependent on the services they offer (Deshefy-Longhi, et al., 2004).

The health care context with respect to EMR use and management in primary health care facilities is the intended focus of this study. The literature will therefore address how effectiveness and efficiency can be established when dealing with the privacy rights of patients. The intention is to ensure that their privacy rights are maintained throughout the confidential relationship and that the accessibility to the EMR within the primary health care facility meets privacy compliance requirements.

Privacy is considered a philosophical concept that is not easily defined, and is therefore not easily understood by most (Nissenbaum, 2010; Nippert-Eng, 2010; Solove, 2008; Margulis, 2005; Introna & Pouloudi, 1999). To this end, much research has been done to try and reach an understanding of the aspect of privacy associated with information, i.e. information privacy (Smith, et al., 2011; ISTPA, 2007). The nature of privacy is addressed in this study in order to determine a working definition of privacy that can be used to understand the privacy legislation (Corliss, 2010; Westin, 1967).

To further understand the nature of information privacy, the concept of personally identifiable information (PII) is investigated with examples drawn from the Protection of Personal Information (PoPI) Bill of 2009 (SA Justice Dept, 2009). An example of the typical life cycle of PII is demonstrated in the discussion on information privacy (ISTPA, 2007; ISTPA, 2002). The foundational elements of privacy legislation, namely the Fair Information Practices (FIPs) are introduced and discussed in relation to various privacy instruments identified (ISTPA, 2007). This discussion aids in identifying the common principles associated with privacy legislation. The PoPI Bill is further explored and the ISO/IEC 29100:2011(E) standard is introduced and forms an integral part of the development of the artefact for this study.

Confidentiality is discussed by reaching an understanding of its nature (McCallister, Grance, & Scarfone, 2010; Whitman & Mattord, 2009; Agrawal & Johnson, 2007; Deshefy-Longhi, et al., 2004). The notion of how collective privacy boundaries are established between the patient and the health care practitioner is explored (Petronio & Reierson, 2009). The various constraints on the maintenance of confidentiality are discussed with specific concern for the relationship between the patient and the health care practitioner. The difficulties in maintaining a relationship through various zones of contact is also explored (Veeder, 2007; Whetton, 2005). The expectations of trust are discussed as a determinant of the level of confidence the patient is willing to place in the health practitioner (Earle & Siegrist, 2008; Huang & Fox, 2006; O'Hara, 2004; Falcone & Castelfranchi, 2001; Das & Teng, 1998; Mayer, Davis, & Schoorman, 1995). The significance of control in the confidential relationship is discussed (Huang &

Fox, 2006; Flowerday & von Solms, 2006). The expectant predictability of the controls (either formal or social) in existence in the primary care facility are discussed with respect to their significance to interacting with the EMR (O'Hara, 2004; Das & Teng, 1998). However, violations of confidentiality can occur (Petronio & Reierson, 2009; Deshefy-Longhi, et al., 2004; Falcone & Castelfranchi, 2001). The discussion of the problems encountered specifically in a primary health care setting are identified (Williams, 2008). Examples of regulations that address confidentiality are presented, namely: the Caldicott Principles (Keyser & Dainty, 2005) and the HPCSA Guidelines for Confidentiality (HPCSA, 2007).

Accessibility is discussed from the perspective of the concern for information privacy (CFIP) (Smith, Millberg, & Burke, 1996). This discussion is focused on the impact on the *collection of information* (Whitman & Mattord, 2009; Petronio & Reierson, 2009; Whiddett, Hunter, Engelbrecht, & Handy, 2006), *information quality due to errors* (Whitman & Mattord, 2009; Terry & Francis, 2007; Agrawal & Johnson, 2007), the *unauthorised access to information* (Ponemon Institute, 2012; Terry & Francis, 2007; Lederman, 2005), and the secondary uses of information. Socio-Technical Theory (Bostrom & Heinen, 1977) is used throughout to frame the discussion and the focus is on the social perspective. The discussion highlights the threat that individuals with limited understanding of the compliance considerations and information security can pose to the primary health care facility and the information asset (electronic medical record). The requirements for a security culture are presented as a means to assist in raising the awareness of compliance issues (Ciampa, 2010; OECD, 2002).

To assist in framing the discussion, the Theory of Communication Privacy Management (CPM) (Petronio & Reierson, 2009; Petronio, 2002); the Theory of Restricted Access; the Theory of Control; and, the Theory of Restricted Access/Limited Control (Tavani, 2008) are used throughout this research project. These theories have relevance to the discussion on privacy, where an individual seeks to restrict access to their private information; and, with respect to confidentiality, where the amount of control an individual has over their private information once it is shared is considered to be either limited, or not limited at all.

The main focus of the theories is then to address the tension that arises between *privacy* and *confidentiality*, and how people make choices about what private information can be made *accessible* to others. This has implications for the consent provided by patients and the disclosure of information by confidants.

The Theory of CPM provides five principles that seek to understand the dialectical tension between information privacy and its disclosure (Petronio & Reierson, 2009; Petronio, 2002). These principles are listed in Table 1.1 and related to the associated literature chapters where the premise of the principle is discussed.

Table 1.1: Principles of Communication Privacy Management Theory (adapted from Petronio & Reierson, 2009)

CPM Core Principles	Discussed in:
Principle 1: Ownership and control of private information People believe that they own and have a right to control their information.	Chapter 2: Privacy
Principle 2: Rules for concealing and revealing People control their private information through the use of personal privacy rules.	Chapter 2: Privacy Chapter 3: Confidentiality
Principle 3: Disclosure creates a confidant and co-owner When others are told or given access to a person's private information, they become co-owners of that information.	Chapter 3: Confidentiality
Principle 4: Coordinating mutual privacy boundaries Co-owners of private information need to negotiate mutually agreeable privacy rules about telling others.	Chapter 3: Confidentiality Chapter 4: Accessibility
Principle 5: Boundary turbulence – relationships at risk When co-owners of private information do not effectively negotiate and follow mutually held privacy rules, boundary turbulence is the likely result.	Chapter 4: Accessibility

The information privacy principles associated with the Theory of Restricted Access, the Theory of Control, and the Theory of Restricted Access/Limited Control provide a means to focus how individuals negotiate their choices with respect to restricting access and limiting control (Tavani, 2008). The Theory of Restricted Access is concerned with the ***ownership of privacy*** and how the individual provides access to

their private information based on given contexts (Tavani, 2008). Chapter Two discusses the various aspects of informational privacy and how the individual restricts access to their person. The Theory of Control determines that one's privacy is directly proportional to the level of control the individual has over their private information. It is also concerned with ***defining the relationships*** that exist with others in order to maintain that control (Tavani, 2008). Chapter Three is concerned with the establishment of confidentiality based on the amount of perceived trust in a given relationship. This in turn affects the level of control that the individual has over their private information. Finally, the Theory of Restricted Access/Limited Control is concerned with the privacy that an individual has in a situation based on the circumstance contained therein, i.e. the restricted access is concerned with the concept of privacy, and the limited control is associated with the management of the privacy for ***accessibility*** (Tavani, 2008). Chapter Four is concerned with how the various parties gain and manage the access to information.

The next section introduces the methodology followed to collect and analyse the primary data for this study.

1.7. Research Methodology

The interpretive paradigm was chosen at the outset for the research project and compared against the positivist and behavioural science / Design Science hybrid paradigm. Thereafter, the quantitative, qualitative and mixed approaches to research design were discussed and the qualitative research approach was chosen for this research study. A discussion of the strategy of inquiry that was to be utilised to conduct and manage the research project, namely the Design Science research guidelines is discussed. From the discussion, it was evident that the Design Science research guidelines could adequately inform the process needed to develop the artefact for this study.

The use of interviews and an expert review process (based on the principles of the Delphi technique) were investigated and found to be suitable means for detailing the

research process for the research project. Finally, the credibility of interpretive research as a means of credible data collection was discussed, and criteria provided for evaluating the quality of the data.

1.7.1. Data Collection

Semi-structured interviews were used as the means to collect primary data for this research project. The open-ended questions for the interviews were derived from the literature and refined following a process to develop the interview guide (*cf.* Section 5.5.1). The *interview guide* (*cf.* Figure 5.6) allowed for consistency of the administered questions across respondents. The respondents comprised seven experts who had expertise in one or more of the following fields: health care, information security, and privacy (*cf.* Table 5.4).

An iterative expert review process was used for the research process, which comprised three phases of interviews. Three experts participated in individual interviews in Phase One and responded to two *(questions 1 and 8)* of the eight questions listed on the interview guide, i.e. the questions addressing privacy compliance and the proposed artefact (initial model) developed through the literature review. The focus of Phase One was on the *aspects of privacy*. Phase Two involved four experts who participated in individual interviews and answered all the questions listed in the interview guide. They also provided comments on the initial model. The focus for Phase Two was on the *impact of information security on health care*. Phase Three was conducted as a form of focus group where three experts, who had previously participated in Phase Two, were interviewed as a group. The specific focus of Phase Three was on the *refinement of the privacy model*, but also involved clarification of summarised points raised in Phase Two from the presented questions on the interview guide.

After each phase of the iterative expert review process research process, the responses from the experts were collected and analysed. The data analysis from each phase informed the next, and allowed for iterative changes to be made to the initial conceptual model constructed from the literature.

1.7.2. Data Analysis

The data collected *(expert responses)* from each phase of the expert review process were analysed in terms of the responses, and coded using the principles of the ISO/IEC 29100 standard as themes (ISO/IEC 29100, 2011). The responses to Phase One were analysed separately from those of Phase Two and Three, as Phase One only addressed two questions from the interview guide. The responses collected during Phase Two and Three were discussed in terms of the presented themes used for the coding exercise. Each theme detailed the underlying concept associated with it, and provided quotes from the collected responses. Where applicable comments were made at the end of each theme about the model, and related to the layout of the specific iteration of the model presented to the respondents. These comments assisted in refining the proposed information privacy model as presented (*cf.* Section 6.3).

1.8. Delimitation of the Study

This research project focused on the creation of a conceptual information privacy model for use in primary health care facilities with the aim to improve patients' and health care workers' understanding of privacy compliance. In conducting this research project, the following assumptions were made:

- An EMR is localised to a primary health care facility, which is represented by a general practitioner's office, clinic, or hospital;
- The aspect of increased off-site access of the patient to their records is not considered;
- Primary health care research conducted outside the borders of South Africa can be generalised, as there are universal similarities in the manner that medical records are managed;
- Legislation promulgated outside the borders of South Africa has reference where it has informed the development of the legislation in

this country, or details examples specific to privacy and/or health care that provide a contrast of South Africa to other countries; and,

- South African legislation promulgated (Acts) or tabled (Bill) are limited primarily to the incorporation of the Protection of Personal Information (PoPI) Bill of 2009 as a future privacy omnibus legislation, and this in no means implies a diminishment of the importance of any other legislation detailing aspects of information privacy.

1.9. Ethical Considerations

This research project focused on the development of a model, which was initially derived from a review of the existing literature. The respondents (experts) who participated in this research project were provided with information about the focus of the study, so that they could make an informed decision for consent to participate in the study. During the interview process, the experts were advised that they were under no obligation to answer any given question and could opt-out of answering if they so desired. Furthermore, the experts were advised that their responses would be confidential, and advised that anonymity was the accepted practice in the research write-up unless they requested to be identified by name in the research.

1.10. Outline of the Research Project

This dissertation is comprised of seven chapters. *Chapter One* provides an overview of the research project, which includes much of the original proposal for this research. The proposal detailed the problem area, objective, main and sub-research question, research methodology, delimitation of the study, and ethical considerations. A brief summary of the literature review conducted in this research project is also included in this chapter.

Chapters 2, 3, and 4, detail the literature for this research project within a health care context. *Chapter Two* provides a philosophical discussion of privacy and the associated

legislation and standards. The ownership of privacy rights by individuals and their ability to restrict access to their PII is implied throughout the discussion. *Chapter Three* interrogates the notion of establishing collective privacy boundaries for confidential relationships to exist and continue. Trust and controls are discussed with respect to their impact on confidentiality. The expectation of complete control that individuals perceive they have over how confidants protect their privacy is addressed. Examples of legislation informing confidentiality guidelines are explored. *Chapter Four* addresses the various concerns associated with the access to PII. It considers the ability of the individual to restrict access, but also highlights that individuals have limited control over how their PII will ultimately be protected. The importance of finding ways to improve the understanding of protecting information is also addressed.

Chapter Five provides an overview of research paradigms in order to inform the choice of interpretivism as the research focus. The Design Science research guidelines and an expert review process based on the principles of the Delphi technique are explained in relation to the research project undertaken. Furthermore, the research process that was followed to collect the relevant research data is discussed.

Chapter Six analyses the data (expert responses) received during the data collection process and indicates how these responses informed the creation of the model. The final information privacy model is explained.

Chapter Seven provides a conclusion of the research project by reviewing the literature contributions and outcomes against the research question. Details for future research are included.

1.11. Chapter Summary

This chapter provided the roadmap for this study. It detailed the reason for the study and identified the problem to be addressed. The problems discussed in the literature and investigated throughout this dissertation to determine how an improved awareness of the constituents of privacy compliance will influence how patients and

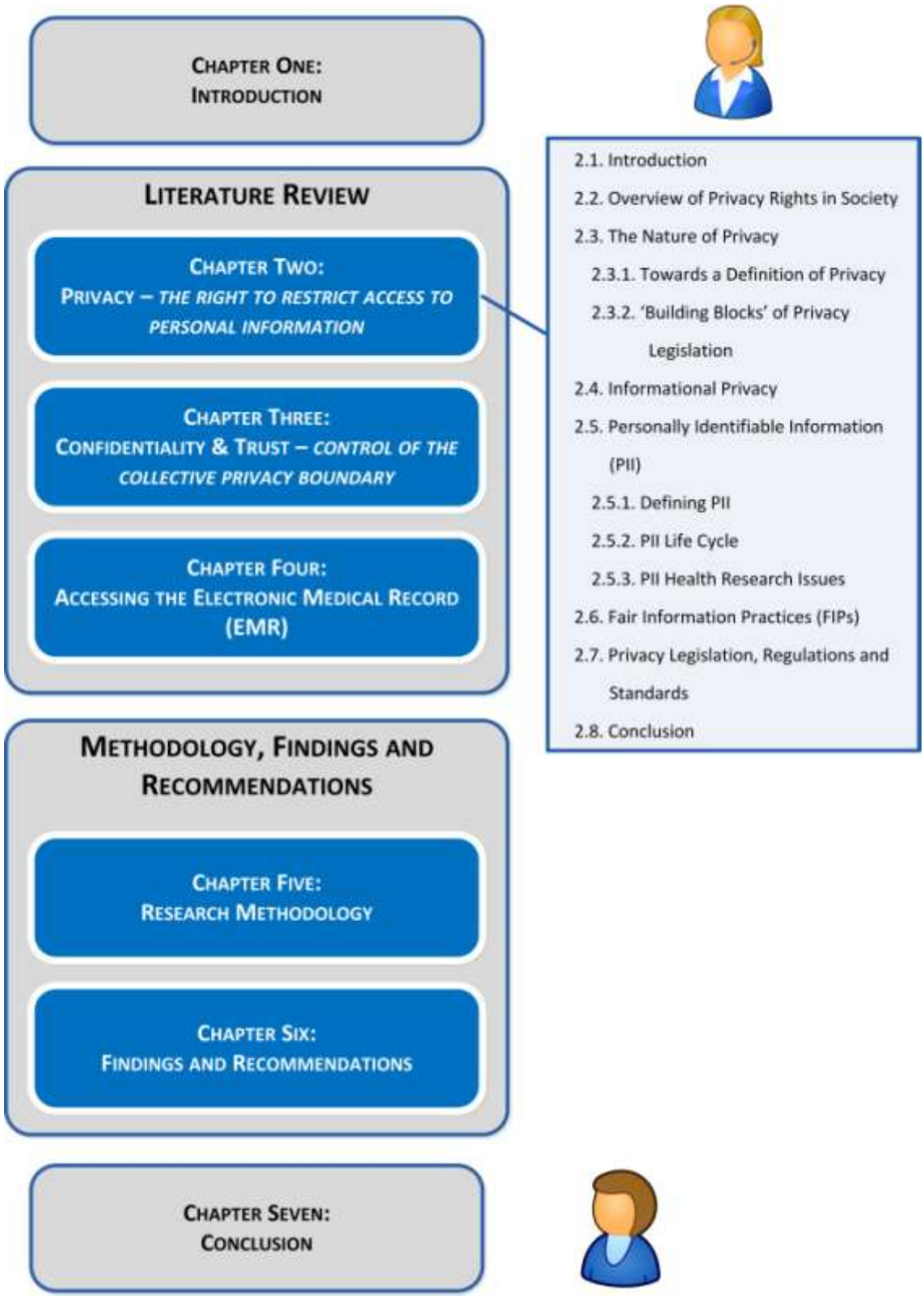
health care workers concern themselves with issues surrounding privacy, confidentiality and accessibility.

The literature to be discussed is summarised in this chapter as well as the theoretical underpinnings that provided the framework for the discussion. The literature informs the research methodology (data collection and analysis) that were introduced in this chapter and expanded on in the dissertation. The delimitations with respect to this study are presented in order to set the context of the study.

The findings for this research project indicated that the privacy compliance landscape is complex, but it is possible to derive a better understanding of privacy by considering the various constructs and creating a visual representation. The intention of the study was not to prescribe the practical aspects associated with meeting the compliance requirements, but rather to provide a model that will residually improve awareness of the existent privacy constructs found in legislation, regulation and standards.

The next chapter investigates the multidisciplinary and philosophical underpinnings of privacy in order to set the foundation for this research project.

CHAPTER TWO: PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*



2.1. Introduction

An investigation of the term '*privacy'* is required in order to establish the foundation for this research project. To this end, this chapter considers the nature of privacy through a brief investigation of multi-disciplinary privacy literature and arrives at an appropriate understanding of informational privacy. Pertinent to an understanding of informational privacy is a discussion of the type of information that needs to be protected, namely personally identifiable information (PII). Thereafter the chapter introduces the PII Life Cycle (ISTPA, 2002). An example of the impact of PII disclosure within the area of medical research is detailed, which has later bearing on the concepts of confidentiality and trust (*cf.* Chapter Three). The Fair Information Practices (FIPs) (Solove, 2008; ISTPA, 2007) are introduced to provide the foundation for the discussion on the Organisation for Economic Co-operation and Development (OECD) privacy principles (OECD, 1980).

The chapter includes a cursory reference to the comparisons of the privacy principles arising from an in-depth analysis of 12 privacy-related instruments chosen by the International Security, Trust and Privacy Alliance (ISTPA) (ISTPA, 2007). The OECD Privacy Principles (OECD, 1980), and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (US Health & Human Services Dept, 2003) are included in the analysis and further expand the context of this research project. The principles of the Protection of Personal Information (PoPI) Bill of 2009 (SA Justice Dept, 2009) are provided, and a standard associated with privacy (ISO/IEC 29100, 2011) and health care (ISO/IEC 27799, 2008) are briefly discussed.

The main underlying theoretical premises covered in this chapter are the question of the ownership of PII as identified by Principle 1 of the Communication Privacy Management (CPM) Theory (Petronio & Reierson, 2009) and the ability of the individual to restrict access to PII which is an underlying principle of the Restrict Access Theory (Tavani, 2008). These premises will be implied throughout the discussions covered in this chapter.

2.2. Overview of Privacy Rights in Society

The debate regarding the nature of an individual's privacy rights have increasingly centred on the threats being posed by technological advances (Nissenbaum, 2010; Solove, 2008). For Samuel Warren and Louis Brandeis that technological advancement, circa 1890, was the proliferation of the print media and the advent of the portable camera (Solove, 2008). This was a turnkey moment for privacy, as they argued that the unsolicited capture of an individual's image was to all intents and purposes an invasion of privacy, and that individuals have the right to keep their private lives closeted (Warren & Brandeis, 1890 cited in Solove, 2008). Progressive advances in technology and the advent of digital tracking and monitoring systems[4] are making it increasingly difficult to keep information about ourselves and our actions private (Nissenbaum, 2010).

Private companies and state agencies under the guise of "universal protection for all" are increasingly recording our image and our actions digitally in multiple instances. This premise is no more evident than in the case of closed circuit television (CCTV), because at no point are we explicitly asked to waiver our right to privacy from surveillance whilst carrying out our actions in public. However, private and public authorities are expected to annunciate their intent for surveillance prior to the locale of camera placement. By entering the street, or public area we implicitly consent to being monitored. Therefore, we consciously choose to allow information about our actions to be collected, stored, manipulated, and potentially shared. In part, we trust that those collecting the information will not utilise it to potentially foster an Orwellian 'Big Brother' society (Nissenbaum, 2010). There is the expectation that the information collected will be utilised for our own betterment and residually for society as a whole (Introna, 1997). However, assume that a primary health care facility makes use of CCTV cameras as a means to monitor a patient's treatment in order to later use the footage to train health practitioners. Does this constitute an invasion of privacy, or

[4] For example: Internet cookies, radio frequency identification devices (RFIDs), global positioning satellite (GPS) technologies, closed circuit television (CCTV), and location aware applications.

because the outcome is improved health care does it not fall in an indefinable grey area?

Nissenbaum (2010) would argue that we have fluidic privacy rights when any information collection occurs in the private/public domain until ***contextual integrity*** is articulated. If we assume a health care context, then contextual integrity is concerned with the –

- ***context*** in which the information is utilised (e.g. patient treatment);
- ***informational norms*** (e.g. health care practitioners share information in certain ways);
- ***actors/roles*** associated with the information (e.g. patients and health care practitioners);
- ***attributes*** of the information (i.e. PII) associated with the patient and their treatment plan); and,
- ***transmission principles*** governing information privacy.

A loss of contextual integrity and a violation of informational privacy rights are indicative of an individual's medical information, which they deem as private, being disclosed (made public) either intentionally or unintentionally to others.

The potential *threats* to an individual's medical information are rising due to the revolution within the health care sector towards the mass digitisation of previously paper-based workflows (Scott, et al., 2007; Choi, Capitan, Krause, & Streeper, 2006). 'Threats' are defined as "an object, person, or other entity that represents a constant danger to an asset" (Whitman & Mattord, 2009, p. 40). The information 'asset' in the context of this research is the EMR of a patient. These threats are contextually dynamic and are often attributed to or perceived to be the cause of, a loss of informational privacy arising from information disclosure.

The disclosed information could potentially be utilised for nefarious purposes, which may threaten the affronted individual's person, property or reputation (Solove, 2008).

Ironically, individuals often lack the awareness or concern of their privacy rights over their information until it has been lost (Nissenbaum, 2010; Introna & Pouloudi, 1999). This is more evident with digitised information, because the degree of privacy appetite of individuals is often dependent on their perception of the technological efficacy towards the protection of privacy (Deshefy-Longhi, et al., 2004). For example, the implied trust individuals place in privacy-enabled technologies associated with social networking sites (Nissenbaum, 2010). However, this perception can often arise out of technological ignorance. For example, the individual who accepts an application request originating from a 'friend' via a social media site, and subsequently divulges their private information and those of their friends when they add the third party application. Similarly, either patients or those managing the medical records of patients can unintentionally divulge information, which should remain private. This is not to say that some unscrupulous individuals would not intentionally disclose a patient's medical records for personal gain. For example, tipping off the popular media, that a politician or celebrity is seeking specific medical treatment.

The next section will investigate the philosophical origins of privacy, so that the issues and concerns raised in this general overview on privacy will be clearer. An understanding of privacy is needed to develop the research project output, which is an information privacy model that can be used as a means to increase privacy awareness in primary health care facilities.

2.3. The Nature of Privacy

A discussion on privacy is necessary to distinguish between privacy and secrecy. The words 'privacy' and 'secrecy' are considered interchangeable, but their focus is fundamentally different. Privacy can simply be described as being able to withhold information about ourselves from others (Smith, et al., 2011; Whitman & Mattord, 2009). On the other hand, secrecy refers to a group of people keeping information from others, and if that information is disclosed then it could lead to negative consequences for the parties concerned (Nissenbaum, 2010; Solove, 2008).

Secrecy and confidentiality are often similarly defined (Whitman & Mattord, 2009), because both are an extension of privacy, i.e. privacy must exist before secrecy/confidentially can be manifested. However, within military circles, confidentiality and secrecy are defined based on the associated damage that might arise from an information disclosure and documents are either marked *confidential*, *secret*, or *top secret*. The focus of this research project will not extend past the level of confidentiality, as this is the common term associated with keeping patient information secure in the health care context. The remainder of this chapter explores the concept of privacy, and Chapter Three discusses the nature of confidentiality.

2.3.1. Towards a Definition of Privacy

A finite definition of privacy does not easily present itself (Nissenbaum, 2010; Solove, 2008; Introna, 1997; Thomson, 1975). This arises in part because privacy is multi-disciplinary, and has been discussed in multiple contexts (Schoeman, 2007). Whitley (2009) supports this view by stating that various social groups and disciplines have explained privacy in a manner that best suits their interpretations of the concept, so no inherent definition exists.

However, privacy is commonly defined as "the claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7). Altman (1976, cited in Nippert-Eng, 2010, p.3) supported this view of privacy by stating that "privacy is a central regulatory process by which a person (or group) makes himself more or less accessible and open to others". Margulis (2005) states that privacy represents control (either complete or partial) over the transactions between relevant parties, or that autonomy can be enhanced and/or vulnerability minimised.

Margulis (2005) postulates that the control of transactions and the access to information regarding the individual usually revolves around how much individuals are willing, or regulated to share of themselves. This is no more evident than in the health care context where privacy has in the past simply been explained as "the right and

desire of a person to control the disclosure of personal health information" (Rindfleisch, 1997, p. 95). However, in instances such as a pandemic, the private information of the patient may need to be disclosed for the greater good (Smith, et al., 2011).

The health profession relies on access to information regarding the individual, but at the same time fosters the notions of privacy and confidentiality. The question is then the degree of accessibility. Figure 2.1 depicts the constant flux between that which should be held private and made accessible to the public.

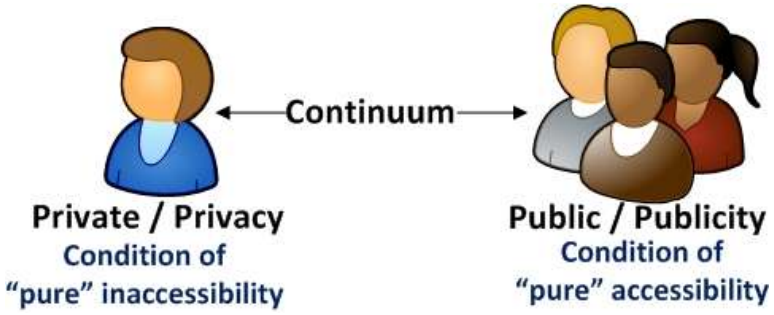


Figure 2.1: Private-public continuum (Nippert-Eng, 2010)

Striving for a condition of "pure" inaccessibility would mean that information about the condition of the patient would only be known to the patient and no other. The patient may not divulge relevant medical complaints due to fear of ridicule (Solove, 2008). Similarly, a patient may deem it inappropriate to allow for "pure" accessibility, which instead would allow all their medical information to be shared with the public collective. Each of the instances of purity marks an absolute on the private-public continuum (Nippert-Eng, 2010). The context and the active elements acting therein and thereon determine vacillation points, and in some instances a point of rest on the continuum. This amplifies the complexity of defining privacy, because no singular rule applies to all contexts, so prescribing universally fixed points and outcomes on the private-public continuum is myopic. Consequently, the dichotomy of what constitutes private or public information about a person has resulted in a series of legal interpretations of privacy in order to arrive at some form of governing principles and understanding of the discipline. However, to gain a better insight into the impact

privacy has on the legal perspective, it is important to consider the legal 'building blocks' of privacy.

2.3.2. 'Building Blocks' of Privacy Legislation

An understanding of what constitutes privacy within the legal perspective (and residually as a whole) requires that it is increasingly analysed either from the perspective of *coherence* or *distinctiveness* (Corliss, 2010). Coherence refers to whether there are common characteristics, or traits of privacy concerns. Whereas, distinctiveness refers to whether privacy interests should be defended as privacy issues, or whether they are better defended in terms of other recognised interests, i.e. if we omit privacy from the equation would we lose something significant (Prosser, 1960). Therefore, if the argument is for distinctiveness over coherence, then the right to privacy is nothing more than a specific grouping of the legal rights that seek to protect privacy (Nissenbaum, 2010; Thomson, 1975; Prosser, 1960).

Prosser (1960, p. 107) proposed that the right to privacy can be simplified into four torts, or harms, of privacy violation. These are the right to be free from:

- ***intrusion*** upon one's seclusion, solitude, or private affairs;
- ***disclosure*** of embarrassing private facts about oneself in public, which would be offensive and objectionable under the '*reasonable expectations of privacy test*[5]' ;
- ***defamation*** of character arising from having "private facts" misrepresented in public; and,
- identity ***appropriation*** or theft for personal gain by others.

[5] Winn (2008) provides an indepth discussion on the notion of a 'reasonable expectation of privacy', and the associated 'test' is depended on if 1) you actually expect privacy, and 2) your expectation is one that society as a whole would think is legitimate. Privacy was again reduced to a right, but one that was context specific. This distinction was important, because it implies the privacy of the person, and not the place.

Prosser (1960) pointed out that the four privacy invasion types (privacy harms) listed above may be subject to different rules and applicable interpretations. Corliss (2010) provides an explanation of the interrelatedness of Prosser's four privacy harms. Firstly, *intrusion* and *disclosure* refer to the invasion of something secret, secluded or private and pertaining to the individual; whereas *defamation* and *appropriation* do not. Secondly, *disclosure* and *defamation* are dependent on publicity; but this is not the case for *intrusion*, but it is implied for *appropriation*. Thirdly, *defamation* represents a falsity or fiction being fabricated; whereas *intrusion*, *disclosure* and *appropriation* do not. Finally, *appropriation* represents personal gain derivation by another; but this is not a consequence (although it might be a contributing factor) for *intrusion*, *disclosure*, and *defamation*.

Bloustein (1964) rejected Prosser's simplification of privacy to mere inhuman harms, and thereby distinctiveness. Bloustein rather supports the notion of coherence, because he proposes that each of the four harms identified by Prosser have significant implications for human dignity, or result in dignitary harms. The discussion of privacy as violating dignitary harms is a major theme that has raged in the ongoing privacy debate (Corliss, 2010; Nissenbaum, 2010), and often compounds privacy rulings (Solove, 2008).

Thomson (1975) supported the notion of distinctiveness in its purest form by rejecting the concept of a right to privacy insofar as she argues that "privacy" in and of itself brings nothing unique to the fore. She substantiates this view by stating that invasions of privacy can be relegated to other more fundamental rights entrenched in law, such as property law, whether that is intellectual or physical property.

Additionally, Introna (1997) proposes that rather than becoming embroiled in a philosophical, political, or otherwise inherently all-consuming discussion of privacy, it might instead be more beneficial to rather consider the actual functioning of privacy. Barth (2008) supports this view by stating that business processes, or workflows are important in understanding privacy and the utility *(value)* associated therewith. To

understand the actual functionality of privacy, Introna (1997) summarised his discussion of privacy into three broad categories, namely:

- privacy as the right to solitude;
- privacy as the right to control information disclosure about the self; and
- privacy as the right to not be the subject of prejudice, ridicule, defamation, or unsolicited scrutiny.

The three identified categories are a hybrid of the torts identified by Prosser (1960) and the later extrapolation by Westin (1967) into the functionality of privacy, namely: informational privacy. The concept of informational privacy is covered in more detail in the next section as it is a tangible component in the discussion of the FIPs, which are addressed later.

2.4. Informational Privacy[6]

Prior to embarking on an explanation of information privacy, it is necessary to ensure a common understanding of the concept of *information*. At the outset, this would seem a simple task, but various disciplines have assigned different meanings to the concept of information. Losee (1997, p.6), in his extensive analysis of a definition for information, stated that "a good definition or theory of information both describes factually what occurs or what exists, as well as provides an explanation of events". Therefore, "information is always informative about something, [whether it is considered] a component of the output or result of the process" (Losee, 1997, p. 8).

The information systems discipline ascribes to this notion, that there is simultaneously an interaction of elements and forces in action on information. This concept is represented by utilising the standard notation of Systems Theory, namely: **Input → Process → Output**. This notation is depicted in Figure 2.2. The data, i.e. alphanumeric

[6] The terms 'informational privacy' and 'information privacy' are used interchangeably throughout the literature relating to privacy. This research project makes use of "information privacy", except when discussing the philosophical concepts where "informational privacy" is more commonly used.

characteristics about a person, place, or thing are input into the system. For the captured or recorded data to have informational value, it must be processed, which involves organising, transforming, and presenting it in a way that gives the data meaning (Shedroff, 1999; Losee, 1997). The output takes on the form of knowledge when the information is used for some action, and it is only then that the information is considered meaningful and useful. Shedroff (1999) points out that if the information cannot be used in some form of understandable communication, then it should simply be considered as useless information, and therefore not meaningfully processed data. This implies that the data was processed incorrectly, or the means utilised were not suitable for the context. Once the processing has occurred, the actors in the given context have access to the information in the form of a given output. The output may be represented in soft copy format, i.e. to the screen of an electronic device, or in hard copy format, i.e. printed documentation. The output may also be the automated input to another system. Losee (1997) points out that once information has been represented as some form of output, it is not always easy to reverse engineer to the original data. This is in part because information is derived within a given context as depicted in Figure 2.2. Although, information is determined for a given context, it is also influenced by the privacy constraints associated with that context.

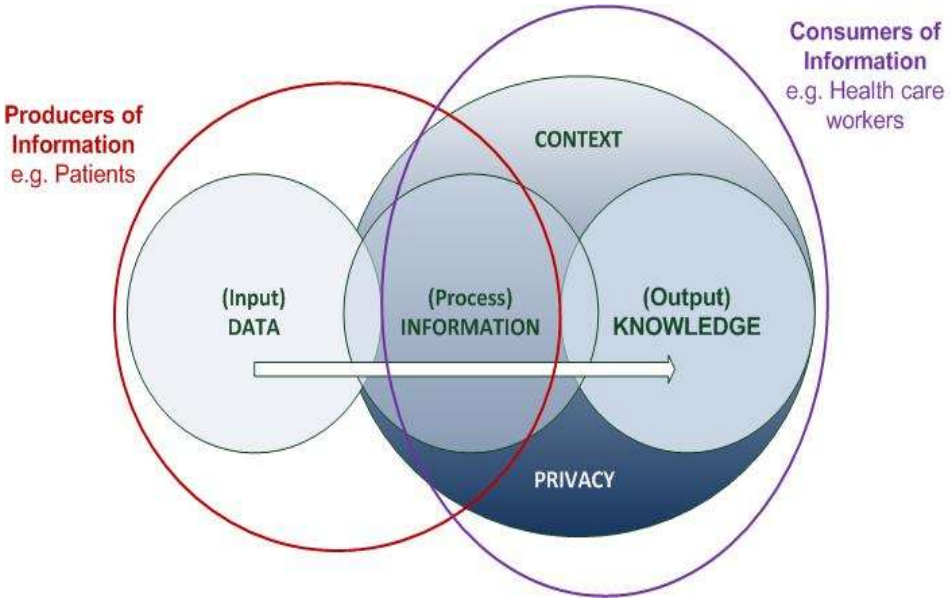


Figure 2.2: Explaining information (adapted from Shedroff, 1999)

Shedroff (1999) believes that information serves as an overlapping point between the producers of information and the consumers of information. The *producers of information* within the health care context are the patients from whom data is collected in order to process it for inclusion in their patient record. The patient record is the information about the patient. The patient has the implied right to determine how, when, where and why their information will be shared. Therefore, the producers of information would believe they exert restricted access over the data and control over the information spheres (Tavani, 2008).

Health care workers are considered the *consumers of information*, because they need to be able to make decisions about the treatment plans for their patients. They make these decisions based on the knowledge, which they have accumulated from their previous experiences. However, they do not automatically have access to information, because of the patient's control over their own information, so they face restrictions in how the information can be shared with others. Therefore, the consumers of information can be said to exert limited and authorised control over the information sphere, but are seen to have complete control over the knowledge sphere (Tavani, 2008; Shedroff, 1999).

The key element is the control of the information by the producers of information who will ultimately decide how much information they are willing to disclose. Westin (1967) argued that privacy is not purely the notion put forward by Warren and Brandeis for the "right to be let alone", i.e. free of nuisance. He believed that privacy should primarily be seen as the control of information, which in social contexts is expressed by an individual's right to withhold themselves from interaction with others. The key constructs of Westin's concept of informational privacy have been depicted in Figure 2.3.

Westin's (1967) informational privacy is concerned with the amount of control an individual exerts on their information to keep it private, as opposed to their degree of social participation, i.e. how much they are willing to make public. The amount of control that an individual exerts on their information is determined by the social

context in which they find themselves (Nissenbaum, 2010). *Solitude* refers to that individual who does not want to share any information with another. They are in a state of absolute privacy, or pure inaccessibility (*cf.* Figure 2.1). *Reserve* implies that individuals decide to keep certain information private from everyone else, i.e. information that is not shared for fear of repercussions. *Intimacy* is concerned with the control individuals exert on the information they are willing to disclose to others. Intimacy and reserve sound very similar, but reserve is concerned with the amount of control exerted on keeping information private, whereas intimacy is concerned with the control associated with sharing information, or making it public. *Anonymity* is concerned with controlling what information is associated with the individual, i.e. information, which is in the public domain cannot be traced back to the individual.

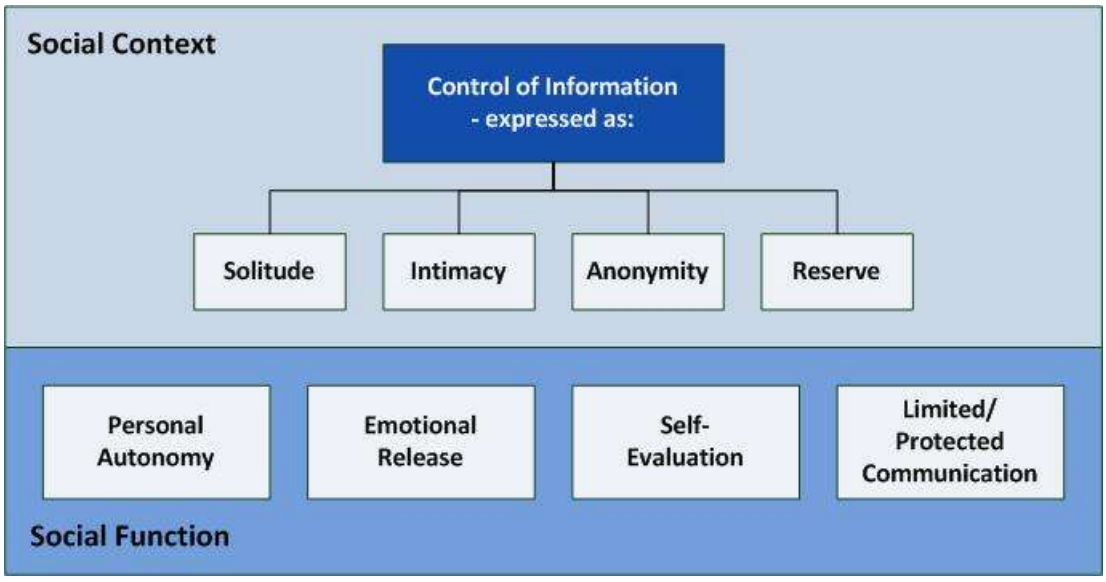


Figure 2.3: Westin's Informational Privacy (designed from literature for this study)

Westin (1967) explained that the justification for the control of information originates from four distinct social functions, which individuals must address in their lives. These are represented in the bottom half of Figure 2.3. *Personal autonomy* is fundamental to the individual maintaining their individuality by being the owner of their own decisions. This means that the individual must decide what information to withhold or share without experiencing a threat to the self. *Emotional release* is indicative of the individual being able to manage the sharing of that information which is construed as inappropriate by the greater society. *Self-evaluation* is where the individual evaluates

the information they are receiving from the world, and how their ideas may be interpreted against accepted societal norms. Finally, *limited and protected communications* is concerned with whom individuals feel they can share their information, i.e. who do they trust (*cf.* Section 3.3).

Individuals have a relative amount of control over their information (Solove, 2008). However, their greatest threat to the control of information arises from how much of their information enters the public domain (Nissenbaum, 2010). The anonymity of an individual is always at risk, because the vast flows of digital information make it increasingly easier to identify the individual from whom the information originated (Narayanan & Shmatikov, 2010). Losee (1997) raised a valid point in identifying the difficulty in reverse engineering information to the original data, but he did not discount it from actually occurring. Technological advances have increased the availability of accessing the data from which information was derived (Agrawal & Johnson, 2007).

Definitions of privacy, information, and informational privacy have been discussed. However, before the principles of privacy and privacy related legislation can be discussed it is necessary to explain the concept of PII.

2.5. Personally Identifiable Information (PII)

Information about individuals is becoming increasingly more accessible with advances in technology (Nissenbaum, 2010; Bennett & Raab, 2006). This accessibility occurs not only from the digitisation of paper-based records, but also from information generated from the storage of biometric information (Crompton, 2003) and DNA sampling (Rosen, 2003). Biometric information such as fingerprint, retinal, and facial scans are increasingly utilised for access controls to systems and passport controls. With respect to passport controls, that information is then available to numerous governmental agencies through centralised databases. DNA sampling privacy concerns have increasingly been raised with respect to keeping centralised databases of those transgressing the law, and for medical research. Rosen (2003) cautions that once this

information is collected and stored in central databases, that it could be utilised towards a number of ends. This concern is highlighted with the aid of the following scenario of DNA usage:

> Consider a scenario where you enter a fast food outlet, and a medical researcher asks you if you would be willing to participate in a short medical survey to assist in mapping the eating habits of individuals. You have to wait for your order anyway, so you agree to participate, and sign a consent form. Part of the survey includes a DNA sample, which you have no qualms giving as you routinely give them before participating in triathlons. Now consider further, that ten years later you apply for life insurance, and provide a DNA sample as part of the medical examination. The insurer does a search on your DNA, and finds that you were involved in a nationwide study that concluded people who visit fast food outlets have a higher likelihood of heart attack and diabetes. On these grounds, they deem you a high-risk candidate, and deny your life insurance.

It would appear from the scenario that being able to keep information private may be a very arduous task when DNA is thrown into the mix. The fast food scenario raises another concern as to where, when, and how our information is being utilised. The retention of information and the access thereto is of great importance, especially in the case of medical related information.

Gostin (1997, p. 684) warned that the "[e]stablishment of an extensive infrastructure of health care information would create countless opportunities for invasion of privacy by the many authorised users, users who have lawful access without explicit authority, and users who obtain fraudulent access". Therefore, it is for this reason that we need to clearly define what is meant by PII, and how, if at all, it can be controlled.

2.5.1. Defining PII

Narayanan and Schmatikov (2010, p.24) argue that "for a concept that is as pervasive in both legal and technological discourse on data privacy, PII is surprisingly difficult to

define". The Protection of Personal Information (PoPI) Bill of 2009[7] (pp.7-8), currently completing the process to becoming an Act within the South African legislature, defines personal information quite extensively as "mean[ing] information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

[7] The two Information Bills currently (circa 2012) under review in the South African Legislature are the ***Protection of Information (POI) Bill***, and the ***Protection of Personal Information (PoPI) Bill.*** The similarity of the names is cause for confusion, because the POI Bill *(also referred to as the Secrecy Bill)* deals with the degree of control the State has over information shared (transparency) with the public. The PoPI Bill originated to address the European Union requirements for the protection of trans-border information flow for its citizens and its companies trading with South Africa. South Africa is a laggard in the adoption of some form of all encompassing Privacy Act to manage all areas of informational flow within the borders of South Africa.

The exclusions specific to the handling and disclosure of medical information are listed in subsection 1 of Section 30 of the PoPI Bill, but are governed by the provisions of subsections 2 & 3 (p.18), which are listed as follows:

> "(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties ***subject to an obligation of confidentiality*** [emphasis added] by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.
> (3) A responsible party that is permitted to process information concerning a data subject's health or sexual life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, ***must treat the information as confidential***, [emphasis added] unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1)".

These exclusions provide for instances when the privacy of the individual may be in conflict with what is considered necessary for the collective good or legal recourse. However, both exclusions listed above attempt to forward the notion of confidentiality, insofar as the protection of PII is concerned. These exclusions aside, the individual has significant control over where, when, and how their personal information is shared. This includes those instances during its life cycle when the individual / data owner / subject are not proximate to said information (ISTPA, 2002).

The PII Life Cycle needs to be elaborated on to explain how PII is utilised in practice. This will assist in laying the groundwork for later discussions focusing on confidentiality (*cf.* Chapter Three) and accessibility (*cf.* Chapter Four). To this end, the next section explains the PII Life Cycle, and thereafter delves further into PII associated with health research, which was introduced briefly in the *fast food scenario* (*cf.* Section 2.5) during the discussion of DNA collection for research purposes.

2.5.2. PII Life Cycle

The ISTPA released the ISTPA Privacy Framework V1.1 in order to provide a common vocabulary and toolkit for dealing with privacy policy development (ISTPA, 2002). This initial framework provided a description of the elements involved in the sharing of PII. An overview of these various elements and their interactions, which provide the basic requirement for the management of PII, is depicted in Figure 2.4. The titles of "Personal Information Preferences", "Consistency", and "Use of Personal Information" are all associated with the expectant proper handling of PII. If PII is properly handled then it is the expectation that privacy management can be realised. To aid understanding, Figure 2.4 is described within the context of a primary health care facility scenario.

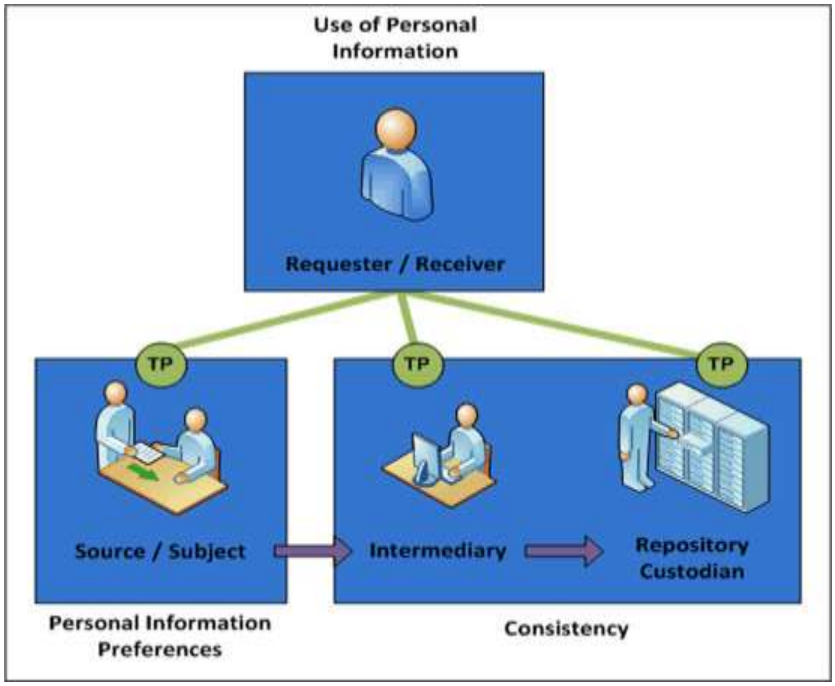


Figure 2.4: PII Life Cycle (adapted from ISTPA, 2002)

The patient (*source / subject*) has a consultation with the doctor, at which time the patient specifies how their PII can be shared. "TP" refers to a touch point or point of interaction, i.e. a point in the life cycle at which an individual, institution or other recognised entity can either request information, or be the recipient of information.

The sharing of the patient's personal information can only occur within the constraints of the personal information preferences stipulated by said patient. The doctor may pass the information onto a nurse (*intermediary*) who then either captures the information electronically, or provides the record to a clerk for capturing. Electronic- or paper-based filing represents the notion of the *repository custodian*. From the initial handover to the intermediary and then onto the repository custodian, there has to be consistency in data management, data security, and data usage. As depicted in Figure 2.4, there can be requests for information regarding the patient. This may be information that needs to be sent to payers (medical aids), specialists, or government departments. In all instances, the patient is deemed, although removed from the proximity of their personal information, to be in control of their privacy.

The overriding assumption is then that the control by an individual over their medical records is largely governed by the degree of privacy they are willing to waiver, i.e. the amount of consent afforded the person holding their records. Whetton (2005) states that the move to the digitisation of medical records is increasingly leading to the acceptance that the patient is now the owner of their medical record, and not the health practitioner, as was the case in the era of paper-based medical records. However, the ease of duplication of digital medical records also raises concerns regarding the control and accessibility thereof, and the importance of consent (Nissenbaum, 2010). Whetton (2005, p.181) states that consent would be required in the following instances, namely:

- health practitioners request access to a patient's record;
- health practitioners are sharing health information with other health practitioners;
- bringing together public health information (e.g. births or cancer registry) with information gathered from individual health encounters; and,
- health administrators, researchers, statisticians, and policy advisers 'mining` health data.

Whetton's final point once again raises the concerns regarding the utilisation of health data for research purposes, where the rights of the individual need to be weighed against those of the public good. Therefore, it seems appropriate to discuss the utilisation of PII within the context of health research.

2.5.3. PII Health Research Issues

Gostin (2001) argues that there is a definite need for the utilisation of research data solicited from medical records towards the greater public good. However, Gostin (2001) stipulates that medical researchers need to adhere to sound ethical considerations in order to ensure that:

- Identifiable data should be collected only when necessary for research;
- Data should be collected and used strictly for scientific assessment of the health care system and other essential public health purposes;
- Researchers should store data securely and allow only those who need access to use such data;
- Secondary disclosures of personally-identifiable data for non-communal goods (i.e. to employers, insurers, commercial marketers) should be prohibited without the individual's informed consent;
- Researchers who violate individual privacy should be severely penalised; and,
- Access to personally-identifiable health data without consent also require impartial, outside scientific and ethical review that weighs the (i) public benefits of the research, (ii) measures taken to protect the confidentiality of the data, and (iii) potential harms to the individual that could result from disclosure.

Damschroder, Pritts, Neblo, et al. (2007) found that increasingly patients wanted the ability to select what portion of their medical information was released for research purposes, i.e. they were in favour of selective disclosure. However, patients believe

that even if consent was provided for one type of research, it should not be assumed that it can be applied indefinitely to all future research (Damschroder, et al., 2007; Woodward & Hammerschmidt, 2003). Hoeyer (2009, as cited in Whitley, 2009), states that the Nuremberg Code[8] specifically allows for the revocation of any consent that was given or implied with respect to participation in medical research.

The South African Medical Research Council[9] (SAMRC) provides the *Guidelines on Ethics in Medical Research: General Principles*, which cites Section 12(2) (c) of the Constitution of South Africa (Act No 108 of 1996) as stating that "everyone has the right to bodily and psychological integrity, which includes the right not to be subjected to medical or scientific experiments without their informed consent" (SA Medical Research Council, 2005). However, the SAMRC also states that in certain instances consent may be provided by a legally authorised individual when the intended research subject is incapacitated and cannot reasonably provide their consent. Ironically, information is often disclosed for medical research purposes within the context of implied consent, as it is often deemed "impractical" to get explicit consent from all data subject holders (Woodward & Hammerschmidt, 2003).

The nature of PII has been determined, and the life cycle of PII described. The dichotomy between information that is private and public was revisited within a brief discussion of information disclosure for medical research purposes.

The next section will further expand on the concept of information privacy by introducing the FIPs, which are associated with the handling of private information.

[8] The judgment by the war crimes tribunal at Nuremberg (post-World War II) laid down ten standards to which physicians must conform when carrying out experiments on human subjects. This code is now generally accepted globally, and forms part of medical ethics.

[9] The South African Medical Research Council Act of 1991 (also known as Act 58 of 1991, which repealed Act 19 of 1969), Section 2, defined the [objectives] of the SAMRC [as], through research, development and technology transfer, to promote the improvement of the health and the quality of life of the population of the Republic and to perform such other functions as may be assigned to the SAMRC by or under this Act.

2.6. Fair Information Practices (FIPs)

The ISTPA provide a detailed chronological account of the origins of the FIPs (ISTPA, 2007). The origin of the FIPs was a set of privacy principles that sought to provide a code of action to address how an individual's private information should be protected (ISTPA, 2007). These were initially contained in the HEW[10] Report, which outlined the following five principles, namely:

- There must be no personal data record-keeping systems whose very existence is secret **[Notice/Awareness]**.
- There must be a way for a person to find out what information about the person is recorded and how it is used **[Choice/Consent]**.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent **[Access/Participation]**.
- There must be a way for a person to correct or amend a record of identifiable information about the person **[Integrity/Security]**.
- Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of data **[Enforcement/Redress]**.

The information practices associated with each of the five principles above are represented by the words contained in the square bracketed items above. These principles would ultimately be the building blocks for the Privacy Act of 1974 (United States), and later global data protection legislation. The next section will review privacy legislation that has relevance to the context of this research project.

[10] The full name for the report is the U.S. Department of Health, Education and Welfare (HEW), Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens circa 1973.

2.7. Privacy Legislation, Regulations and Standards

The ISTPA conducted an in-depth analysis of 12 privacy instruments and were able to identify common privacy principles and practices by carefully reviewing their provisions (ISTPA, 2007). The privacy instruments investigated are listed in Table 2.1.

The privacy principles and practices identified were grouped into a "composite requirement" (main categories), which are represented in Table 2.2. Furthermore, they reviewed the terminology associated with each instrument, and determined what they called a "restructured requirement" (sub categories), which are also represented in Table 2.2. This "restructured requirement" allowed the ISTPA to establish a benchmark of desired requirements for future privacy legislation development.

Table 2.1: Privacy instruments used for an in-depth analysis of privacy (ISTPA, 2007)

Privacy Instrument
The Privacy Act of 1974 (United States)
The OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
UN Guidelines Concerning Computerised Personal Data Files (1990)
Directive 95/46/EC of the European Parliament (1995)
CSA Model Code for the Protection of Personal Information (1996)
Health Insurance Portability and Accountability Act (HIPAA) (1996)
Safe Harbour Privacy Principles (2000)
Federal Trade Commission Fair Information Practice Principles (2000)
Australian National Privacy Principles (2001)
California SB 1386 (2003)
Japan Personal Information Protection Act (2005)
APEC Privacy Framework (APEC) (2005)

Table 2.2: Privacy Requirements Summary (ISTPA, 2007)

Composite Requirement	**Restructured Requirement**
Notice and Awareness	Disclosure; Notice; Openness
Choice and Consent	Accountability; Consent; Collection Limitations; Use Limitations
Access (by the Subject)	Access (Not Correction)
Information Quality	Data Quality; Security / Safeguards
Update and Correction	Correction (not Access)
Enforcement and Recourse	Enforcement

Two of the instruments found in Table 2.1, namely: the *HIPAA Act* and *OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* are briefly discussed as they have had significant influence over the health care industry and global privacy legislation, respectively.

- Health Insurance Portability and Accountability Act (HIPAA)

  HIPAA, a United States health care legislation, seeks to establish efficacy through standardised electronic data transfer associated with administrative and financial transactions in primary health care facilities and their interactions with third parties (Grandison & Bhatti, 2010). Whilst this transfer is occurring, the Act requires that the information is confidential and secure (Grandison & Bhatti, 2010). HIPAA requires that this is accomplished by meeting all of the three standard requirements or rules (Choi, et al., 2006), namely:

  - **Privacy**, i.e. to protect patient data from inappropriate disclosure or use;
  - **Security**, i.e. to establish safeguards around patient information systems thereby preventing unauthorised access; and,
  - **Administrative simplification**, i.e. to encourage interoperability by creating a uniform set of electronic formats, which are specifically concerned with the various *transaction sets* associated with claims,

identifiers (provider, payer, employer, and individual), and *code sets* (diagnosis, therapeutic and treatment).

Problems with complying with the three standards initially plagued HIPAA, because the level of interoperability and move to EHRs has been slow due to health practitioner reluctance and cost implications (Grandison & Bhatti, 2010; Banks, 2006). The Health Information Technology for Economic and Clinical Health Act (HITECH Act)[11] expanded the penalties for compliance with HIPAA due to the anticipated increase in the exchange of electronically protected health information (Grandison & Bhatti, 2010).

Grandison and Bhatti (2010, p. 885) provide a high-level view of the HIPAA Privacy Rule by listing five key principles associated with it, namely:

- ***Notification*** – a covered entity's privacy practices should be made known to patients.
- ***Authorisation and Consent*** – disclosures not permitted under the Privacy Rule need written authorisation.
- ***Limited Use and Disclosure*** – covered entities must use or disclose the minimum necessary protected health information (PHI) for a specific purpose and ensure the development and implementation of policies and procedures governing access and use.
- ***Auditing and Accounting*** – patients have the right to an accounting of all disclosures of their PHI for non-allowed HIPAA operations.
- ***Access*** – patients have the right, under most circumstances, to access the covered entity's designated record set. Covered entities must amend information that is inaccurate or incomplete.

[11] The HITECH Act is part of the American Recovery and Reinvestment Act of 2009 (ARRA), which sought to, amongst other incentives, boost the economy and improve health care by providing finances for a) the establishment of a national health care infrastructure, and b) the accelerated adoption of electronic health records amongst providers (Grandison & Bhatti, 2010).

- OECD Guidelines on the Protection of Privacy & Transborder Flows of Personal Data

  The OECD guidelines (OECD, 1980) included a common privacy framework that stipulated eight privacy principles that needed to be in place in order to safeguard the automated processing of data across countries borders (ISTPA, 2007). The OECD privacy principles are listed in Table 2.3.

  The OECD privacy principles would later form part of the European Commission (EC) Data Protection Directive (Directive 95/46/EC), which are integrated into various privacy legislation throughout the European Union (EU) and influence privacy legislation developments in the Commonwealth Nations (Solove, 2008). The UK Data Protection Act (*cf.* Table 3.1) is an example of such legislation, and it in turn eventually led to the Caldicott Principles (Keyser & Dainty, 2005) (*cf.* Table 3.2), which are discussed in Chapter Three on confidentiality.

Table 2.3: Guidelines for Protecting the Privacy of Transborder Flows of Personal Data (OECD, 1980)

Privacy Principles
1. Collection Limitation Principle
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle
Personal data should be relevant to the purposes for which they are to be used and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification Principle
The purpose for which personal data are collected should be specified not later than at the time of data collection and subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **continued on next page** -

Table 2.3 (continued)
4. Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or, b) by the authority of law.
5. Security Safeguard Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle
An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.
8. Accountability Principle
A data controller should be accountable for complying with measures which give effect to the principles stated above.

These principles have influenced, in part, the various industry sector privacy legislations in South Africa, and are now included in full in omnibus privacy legislation, i.e. the PoPI Bill/Act[12]. The principles included in the PoPI Act are listed in Table 2.4, and discussed further (*cf.* Section 6.3) when explaining the proposed information privacy model for this research project.

[12] The PoPI Bill is expected to be signed into law as an Act in 2013 by the State President. At present, PoPI is referred to interchangeably in the popular media as an Act already.

Table 2.4: Privacy Principles of the PoPI Bill (SA Justice Dept, 2009)

PoPI Principles
1. Processing limitation *applicable to* a. Lawfulness of processing b. Minimality of processing/use c. Consent and necessity conditions d. Collection directly from data subject
2. Purpose specification *applicable to* a. Collection for specific purpose b. Data subject aware of purpose of collection and intended recipients c. Retention of records
3. Further processing limitation
4. Information quality
5. Openness
6. Security safeguards *relating to* a. Security measures to ensure integrity of personal information b. Information processed by person acting under authority c. Security measures regarding information processed by processor d. Notification of security compromises
7. Individual participation *associated with* a. Access to personal information b. Correction of personal information
8. Accountability

Table 2.3 and Table 2.4 reflect the similarity and yet differences that can occur in detailing the principles associated with privacy. These minor discrepancies make it difficult to reach a common consensus of how to get privacy operationalised with the use of ICT. The International Standards Organisation provided the ISO/IEC 29100:2011(E) – *Information technology – Security techniques – Privacy framework*, which provides a common set of terms and expectations for a common understanding of how to apply ICT to the management of privacy associated risks. Table 2.5 details the privacy principles of the ISO/IEC 29100:2011(E). These have not been discussed in this chapter as the principles in Table 2.5 provide the themes for the analysis of the data for this research project and are discussed extensively at that point (*cf.* Chapter Six).

Table 2.5: The privacy principles of the ISO/IEC 29100:2011(E)

ISO/IEC 29100 – Privacy Principles
1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimisation
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

There are a myriad of international legislation related to privacy, which makes it difficult to generalise across legislation. However, the privacy legislation in existence all appears to have similar underlying principles albeit that they are sometimes 'packaged' differently. The specific legislation for a country (e.g. South Africa's PoPI Act); in conjunction with the ISO/IEC 29100:2011(E) could make it easier to gain a greater awareness of privacy in order to get it operationalised.

The international standard ISO/IEC 27799:2008(E), namely: *Health informatics – Information security management in health using ISO/IEC 27002:2005* also needs a brief mention as it operationalised the security standards raised in ISO/IEC 27002:2005 into the health care environment. ISO/IEC 27799:2008(E) does not replace ISO/IEC 27002:2005, but seeks to augment the standard by elaborating on those guidelines to ensure that there is clarity on how they can be interpreted and implemented within health informatics. The ISO/IEC 27799:2008(E) (p. 1) standard is explained as:

> "a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing [it], health care organisations and other custodians of health information will be able to ensure a minimum requisite level of security

> that is appropriate to their organisation's circumstance and that will maintain the confidentiality, integrity and availability of personal health information."

This research project will not explore this standard further, such that its inclusion here serves merely for noting and to indicate that it was not omitted as an oversight. The focus of this research is primarily on privacy compliance. However, where relevant throughout this research project reference has been made to information security when it supported the primary discussion.

2.8. Conclusion

It has been established in this chapter that the philosophical origins of privacy are complex, but at the same time, they have provided a clear definition of information privacy. This was established by considering the various constructs of privacy, defining information, and reviewing Westin's notion of informational privacy.

The significance of personally identifiable information (PII) when considering information privacy was discussed. The various types of PII were highlighted by citing examples from the Protection of Personal Information (PoPI) Bill of 2009. PoPI also identified considerations with respect to confidentiality, which are addressed in Chapter Three to follow.

How PII might be represented in a given setting was discussed by considering the PII Life Cycle presented by ISTPA. This has relevance on two counts; it points firstly to how PII can be depicted, and secondly how it could be managed. The significance is realised later in the study when detailing the proposed information privacy model.

The Fair Information Practices (FIPs) were introduced in order to lay the foundation for the further consideration of the various legislation and instruments associated with privacy. This included providing a review of the ISTPA report on the common and recommended privacy constructs for future privacy instruments. It became apparent from this review that there are a number of common privacy principles, although they

are often packaged/ordered differently in instruments. A further observation is that a given privacy principle cannot be considered in isolation, and that there is an inherent symbiotic relationship between the principles.

HIPAA was briefly discussed as an example of a significant piece of health care legislation that is making significant changes to the provision and protection of health care in the United States. Finally, the chapter listed the principles contained in PoPI, which are revisited in Chapter Six as part of the proposed information privacy model discussion. The international standards, ISO/IEC 29100:2011(E) (on privacy), and ISO/IEC 27799:2008(E) (on health care) were briefly discussed. Much of the literature discussed in this study can be seen as summarised in the ISO/IEC 27799:2008(E), and therefore said standard is not discussed further. The ISO/IEC 29100:2011(E) standard on privacy plays a prominent role in the analysis of the data in Chapter Six.

From a theoretical perspective, this chapter detailed the various issues surrounding the ownership of private information and how individuals make choices about restricting access to their information. This is the fundamental principle of the Restricted Access Theory, and details Principle 1 of the CPM Theory. Principle 2 of the CPM straddles the notions of privacy and confidentiality as it considers how individuals move to a position where they are willing to share information with others by extending their personal privacy boundary.

The significance of explaining the privacy constructs for this research study is to increase an understanding of the compliance landscape, especially with respect to maintaining a patient's privacy rights. Related thereto is the understanding that people have different perceptions of privacy, and that these may not correspond with what is detailed or required by legislation, regulation, and standards. Furthermore, individuals make a conscious choice to share information based on their privacy appetite, which affects the authority they may give to health care workers when allowing access to their electronic medical records. The importance of a health care worker's perception of privacy will impact on whether or not they keep a patient's medical information confidential.

The next chapter considers confidentiality, which is the next step towards reaching a point where the electronic medical records of patients can be accessed by those who need the information to effectively treat the patient.

CHAPTER THREE: CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER ONE:
INTRODUCTION

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

- 3.1. Introduction
- 3.2. The Nature of Confidentiality
- 3.3. Expectations of Trust
  - 3.3.1. Factors of Perceived Trustworthiness
  - 3.3.2. Building and Preserving Trust
- 3.4. Predictability with Controls
- 3.5. Violation of Confidentiality
- 3.6. Regulating Confidentiality
  - 3.6.1. Caldicott Principles
  - 3.6.2. HPCSA Guidelines for Confidentiality
- 3.7. Conclusion

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

3.1. Introduction

Patients expect that private information about them will be kept confidential by health care practitioners (Smith, et al., 2011; Deshefy-Longhi, et al., 2004). This confidentiality can only come into existence if a level of trust has been established between the patient and health care practitioner (Earle & Siegrist, 2008; O'Hara, 2004). Without the establishment of clear boundaries about who can be trusted, patients may be reluctant to give information needed to provide effective and efficient medical treatment (Petronio & Reierson, 2009). This means that patients withhold information from disclosure when they feel it may shame them or lead to ridicule (Nissenbaum, 2010; Solove, 2008). It is these types of personal choices about their privacy rules that determine how much medical information patients are willing to keep private and make public (Petronio & Reierson, 2009; Petronio, 2002), which directly impacts on the level and type of treatment they receive (Damschroder, et al., 2007; Whetton, 2005).

According to Petronio (2002), confidentiality is linked to privacy and the Communication Privacy Management (CPM) theory is a useful means to understand confidentiality. Petronio and Reierson (2009) state that individuals (patients) make decisions about who to accept as a confidant based on their personal privacy rules *(CPM Principle #2).* These privacy rules will then determine how much private information they share with others (health care practitioners) when making them co-owners of the information *(CPM Principle #3).* The patient needs to accept that they need to give consent for the sharing of information in order to be treated (Deshefy-Longhi, et al., 2004). Thereafter, the health care practitioner will share information with their own set of confidants. These new co-owners are expected to be bound by the privacy rules of the patient. Unfortunately, not all co-owners are trustworthy (Falcone & Castelfranchi, 2001).

Those confidants that disclose private patient information to an unauthorised individual threaten the trust that was earned in order to create the confidential relationship in the first instance. It is therefore necessary for those who co-own the

private information to agree on the privacy rules that will be applied when telling others *(CPM Principle #4)*. This relates again in part to the issue of consent, which will be discussed later in this chapter and revisited in Chapter Four.

The principle of the Control Theory is also relevant to the theoretical underpinning of this chapter, as the amount of privacy an individual has is directly proportional to the amount of control they have over their private information (Tavani, 2008). Therefore, when a confidential relationship is being created or is already in existence, it is constantly influenced by the amount of control an individual wants to exert over their private information.

This chapter will discuss the nature of confidentiality, trust and control within the context of health care to indicate how the interactions of patients and health care practitioners are influenced by an underlying notion of privacy. Thereafter, the violation of confidentiality is briefly considered, which can have significant effects on the establishment of trusting relationships. Finally, two examples of confidentiality regulation, namely the Caldicott Principles (Keyser & Dainty, 2005) and the HPCSA Guideline for Confidentiality (HPCSA, 2007) are presented in order to indicate how confidentiality compliance can influence the actions of health care workers.

3.2. The Nature of Confidentiality

Confidentiality can be considered to be a type of information privacy, because it requires information that was private to be made quasi-public[13] (Deshefy-Longhi, et al., 2004). Within health care, confidentiality is generally accepted as meaning that a confidant will not share/disclose private information that has been shared with them (Whetton, 2005). There is also the expectation that the information collected from the patient will not be used for anything other than that for which it was intended (Agrawal & Johnson, 2007).

[13] Quasi-public – refers to private information that has not been made completely public, but requires those holding the private information to enter a new privacy relationship, i.e. become confidants.

The distinction between confidentiality and privacy is in the manner in which access to private information may be achieved (Deshefy-Longhi, et al., 2004). A loss of privacy occurs when there is unauthorised access to your private information (Nissenbaum, 2010). For example, your private diary is read without your knowledge. When private information is disclosed to an unauthorised individual, then a loss of confidentiality is said to have occurred (Whitman & Mattord, 2009). For example, you share a part of your diary with a confidant who has agreed to tell no one, but then they gossip about the contents to someone else without your knowledge. Within the context of this research project, it would mean that the primary health care facility would maintain confidentiality by ensuring that there is no disclosure of personally identifiable information (PII) in such a manner that an individual or an organisation would be adversely affected by the experience (McCallister, et al., 2010).

Furthermore, when confidentiality is established, there is a shift in the information privacy boundary as well as where control is held (Petronio & Reierson, 2009). The 'treatment' boundary is not only isolated to the owner *(patient)* of the information and a singular confidant *(health care practitioner)*, but to multiple confidants within and outside a primary health care facility. Westin (1976, cited in Veeder, 2007) states that the collection and dissemination of personal information can be divided into three "zones" (*cf.* Figure 3.1), namely:

- **Zone 1:** ***Point of primary contact***, where a medical record is created or updated when the patient seeks treatment from a health care practitioner at a primary care facility, and/or where a confidant legitimately shares the information with another confidant;
- **Zone 2:** ***Point of support contact*** – where payers (e.g. medical aids) access patient information to make payments and government bodies access patient information to ensure the quality of care; and,
- **Zone 3:** ***Point of social contact*** – where those not directly involved in the treatment regime access the patient information for research or consumerism (i.e. for financial gain not directly associated with the treatment administered).

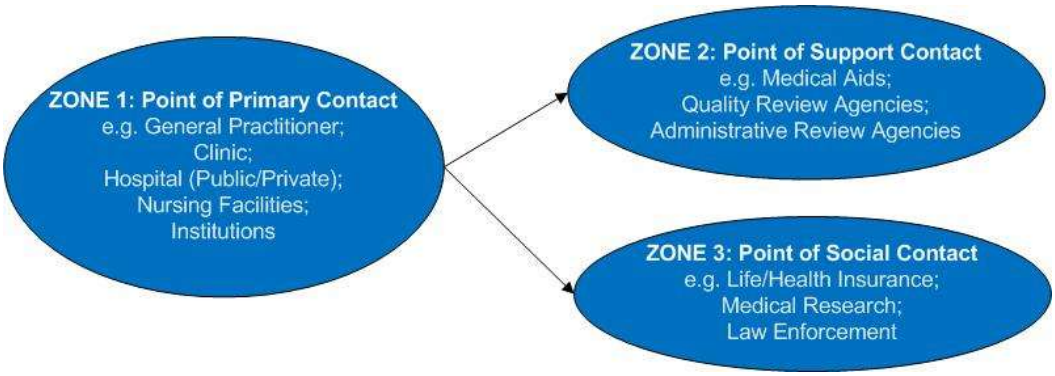


Figure 3.1: Zones of contact in health care (adapted from Rindfleisch, 1997)

The patient's consultation at a primary health care facility generates large amounts of information throughout and beyond the *point of primary contact* with many individuals from multiple locations seeking access to information (Whetton, 2005). It has been estimated that upwards of 400 individuals may have access to a patient's electronic medical information whilst it moves through these 'zones', although not all these individuals are actually involved in the initial treatment or have complete access to all the PII (Veeder, 2007).

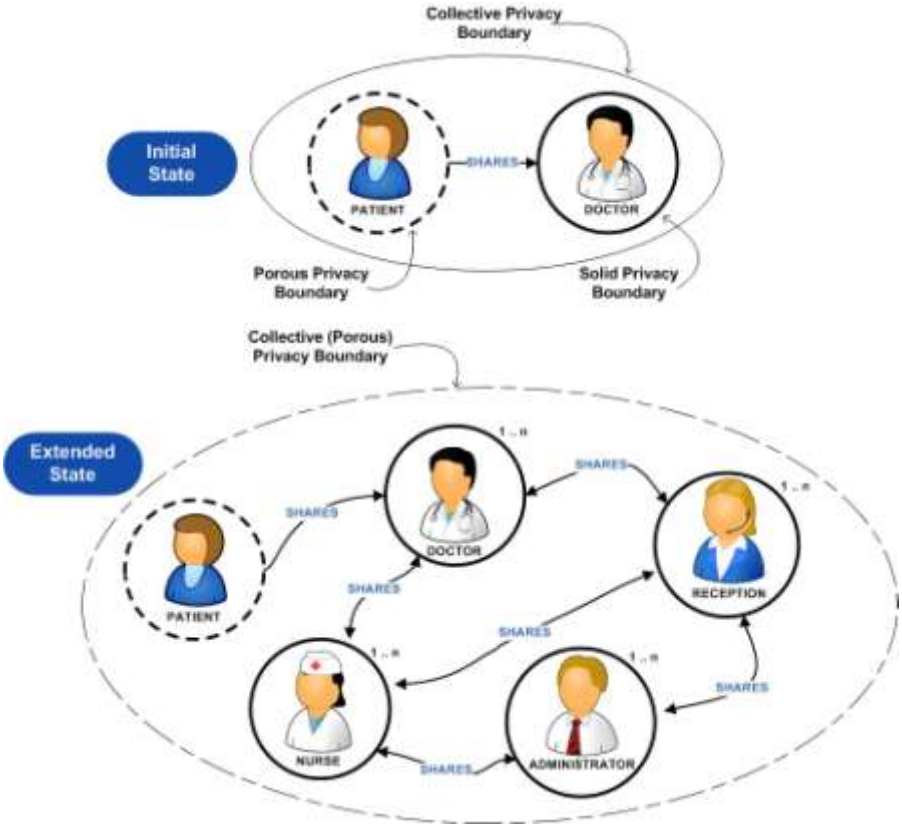


Figure 3.2: Interpretation of collective privacy boundary in primary health care

Patients rely on the establishment of a collective privacy boundary where the personal privacy rules of those individuals in the 'zones' assist in maintaining confidentiality. Figure 3.2 represents the initial consultation of the patient with the doctor. During this consultation, the patient makes a decision to share private information with the doctor and the patient's privacy boundary becomes porous. The doctor's privacy boundary remains solid unless he actively shares his own private information with the patient. However, the sharing of private information is traditionally one-sided, i.e. from patient to doctor. Together the patient and doctor enter a contract of confidentiality and thereby establish a new collective privacy boundary. This represents the *initial state* of the confidentiality. However, the reality is that many individuals could be involved in the treatment process in some capacity/role, so that the *extended state* shown in Figure 3.2 is more often than not an extrapolation of the *initial state*. The *1..n* notation alongside the various roles represents the number of individuals (co-owners) who are being added to the collective privacy boundary. An increase in the co-owner cohort raises the chance of the collective privacy boundary becoming increasingly porous.

Petronio and Reierson (2009) state that as the boundary morphs from one state to the next, it can never return to its original state. Additionally, as the number of co-owners increases various interpretations will arise as to how the private information in their possession should be managed (Petronio, 2002). Those co-owners who did not solicit the original private information or are unsure of its origin will often be more casual about its protection (Earle & Siegrist, 2008). Patients and health care practitioners use various regulations to delegate the care of the private information from one to the other as it moves within the expanding collective privacy boundary (Petronio & Reierson, 2009). Petronio and Reierson (2009) warn that the establishment of a finite number of confidants is preferable, as the setting of parameters for the control of the private information becomes increasingly difficult as the cohort expands.

The sharing of private information within the collective privacy boundary is still fundamentally a product of the establishment of a trusting relationship between a trustor and the trustee (Petronio & Reierson, 2009). Confidentiality relies on the

existence of trust and controls in order to be realised. Therefore, trust will be considered in the next section followed by a discussion on controls.

3.3. Expectations of Trust

Trust is primarily a philosophical construct that describes how we define our identity, our place in the world, and work towards formulating social interactions (O'Hara, 2004; Falcone & Castelfranchi, 2001). More formally, trust is concerned with the cognitive choice to willingly expose oneself to vulnerability based on the expectancy of a desired action by another (Huang & Fox, 2006). There is always an expected outcome attached to trust (Earle & Siegrist, 2008). The level of risk appetite would determine the amount of vulnerability the individual is willing to allow in pursuit of that given outcome (Falcone & Castelfranchi, 2001). Das and Teng (1998) state that trust and risk taking are reciprocal, because as the expected behaviour materialises in the face of a given risk; it strengthens the level of trust. If there is no associated risk and clear outcome expected, then trust will not manifest (Lacey, 2009).

The next section utilises the proposed Model of Trust developed by Mayer et al. (1995) in order to review the process of arriving at an expected outcome. The focus will be on the factors associated with perceived trustworthiness.

3.3.1. Factors of Perceived Trustworthiness

O'Hara (2004) warns that the abstract nature of trust makes it a difficult construct to research and it is therefore necessary that it is considered within a given context. The health care context already presupposes the existence of a trustworthy relationship, because of the underlying principles of the Hippocratic Oath (O'Hara, 2004). Although, it is not the swearing of the oath that makes a person trustworthy, but rather patients and health care practitioners agree to subscribe to a set of common values for the collective (O'Hara, 2004). McAlistair (1995, cited in Das and Teng, 1998) states that

the realisation of the trustee that the trustor has taken a risk associated with their expected behaviour normally makes them act in a trustworthy manner.

Mayer et al. (1995) proposed a model of trust that identified three factors of perceived trustworthiness in a trustee, namely: Ability, Benevolence, and Integrity. These will be briefly discussed in respect of the two roles involved in trust: the trustor and trustee (Huang & Fox, 2006). The trust antecedents are indicated in Figure 3.3.

In Figure 3.3, the ***Trustor's propensity*** refers to the trustor's willingness to trust a trustee (Mayer, et al., 1995). However, not all trustors display the same level of trust in trustees (Oates, 2006), or are willing to trust at all unless there is an absolute guarantee that the outcome they want will be realised (Falcone & Castelfranchi, 2001). Surprisingly there are trustors who increasingly practice blind trust, where the trustor trusts in situations where trust should not implicitly be occurring (Mayer, et al., 1995). An example of this would be the complete trust some trustors place in a doctor without first inquiring about their track record from referring patients. Mayer, et al. (1995) acknowledge that there are variations in the determination of a trustor's propensity to trust a trustee and that these range from being consistent across situations to being influenced by situational characteristics (such as historical outcomes).

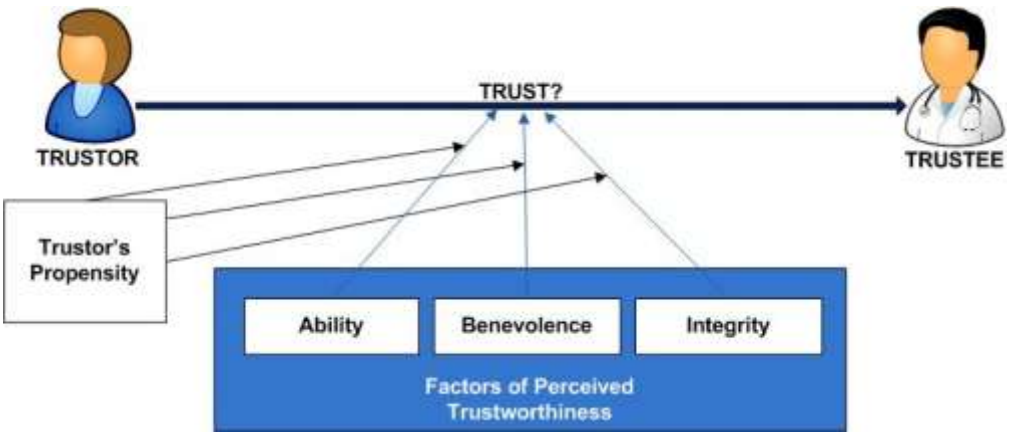


Figure 3.3: Trust antecedents (adapted from Mayer et al., 1995)

The trustor's propensity to trust is influenced by the three factors of perceived trustworthiness. Each of these factors will be briefly considered in relation to the context of health care.

- ***Ability*** refers to a trustee's domain specific influence that is evidenced by their skills and competencies (Mayer, et al., 1995). For example a doctor may be known to be an expert in an illness (e.g. diabetes), but may not be knowledgeable about another area, so would not be trusted in that alternative area.

- ***Benevolence*** is concerned with the notion that the trustee has the best interests of the trustor at heart and this is not driven by an extrinsic reward for the trustee (Mayer, et al., 1995). A patient typically makes the assumption that a health care practitioner is assisting them with their treatment plan, because they want them to get better. For example, a doctor that will extend the hospital stay of a patient to improve his consultation charges does not have the patient's best interests at heart (O'Hara, 2004).

- ***Integrity*** involves the adherence of a trustee to a set of principles that the trustor believes accommodate a trusting nature (Mayer, et al., 1995). For example, the Caldicott Principles adopted by the National Health Service in the UK provide a set of guidelines for confidentiality in primary health care facilities. These principles are expected to be used by health care practitioners when dealing with patients and their private information (Keyser & Dainty, 2005).

Mayer et al. (1995) state that high levels of ability, benevolence and integrity are the ideal for trustworthiness to exist. However, they are separate factors and may not be high all the time (Mayer, et al., 1995). The decision of what level of trustworthiness exists is fundamentally a within-trustor perception of reality, and not necessarily a between-trustor reality (Mayer, et al., 1995). The differences in trustor perceptions

arise when a trustee may be viewed as having a high rating of ability, benevolence and integrity, but this is not a shared view of others. For example, nurses working at a primary care facility may have a low degree of benevolence for a given doctor, although the patient may have a high benevolence based on the limited information they have on the doctor.

Earle and Siegrist (2008) state that the basis of trust is to reach a conclusion that the trustee would act as the trustor would in a given situation. The antecedents of trust discussed with respect to trustworthiness have promoted the idea of shared values (Mayer, et al., 1995). However, shared values, or real trust is built and preserved over time (Lacey, 2009). The next section will briefly consider how trust may be established and preserved within the context of a primary health care facility.

3.3.2. Building and Preserving Trust

It has been established earlier in the chapter that trust is subjective by nature. Therefore it is not surprising that trust can easily be established by association (associative trust) (Huang & Fox, 2006), i.e. *Jill* trusts *Bob*, *Bob* trusts *Kate*, so indirectly *Jill* trusts *Kate.*

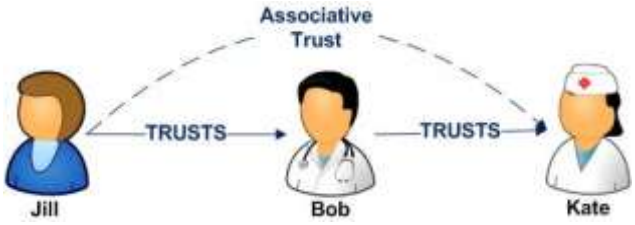


Figure 3.4: Associative trust in the health care setting

However, *Jill* does not trust *Kate* absolutely, but only with some of the matters with which she trusts *Bob*. *Jill* only trusts *Kate*, because *Jill* assumes that *Bob* trusts *Kate*. Lacey (2009) also warns that the differing perspectives and opinions of individuals will determine the extent of trust they have in others, and their willingness to preserve the trust. Flowerday and von Solms (2006) caution that while trust can traverse an intermediary, at the same time it is weakened.

Huang and Fox (2006) state that there are three approaches to the establishment of trust, namely:

- ***Process-based approach*** which relies on past experiences, which consider common values. For example, the *competence* and *honesty* of the health care practitioners; the *security* of the PII to only be used for its intended purpose; and, the *dependability* of the PII that is held at the primary health care facility to be used effectively for a given treatment plan (Lacey, 2009).
- ***Characteristic-based approach*** considers the individual physical traits (e.g. age, culture, gender) that are represented in a common social identity and how they are needed for the eventual establishment of trust (Petronio & Reierson, 2009). For example, there may be cultural differences in the types of treatment plans that patients are willing to consider, or they may have more trust in doctors of a certain age, culture, and/or gender.
- ***Institutional-based approach*** views trust as being established through formalised social structures that are representative of subcultures (e.g. health care practitioners) and intermediary mechanisms (e.g. industry standards and legislation) (O'Hara, 2004).

The establishment of trust is necessary for a patient to allow a permeable privacy boundary to occur, but it is just as easy for that boundary to become solid once more if the patient loses trust in the confidant (Petronio & Reierson, 2009). Once trust is lost, it is not easily recovered (O'Hara, 2004). Therefore, it is necessary to consider how trust may be preserved.

O'Hara (2004) states that the preservation of trust can be accomplished by considering three functions associated with trust, namely:

- **1st Function of Trust – aims to ensure that all individuals are working together in order to realise a common goal**. Through the establishment of open communication and transparent processes by informing the patient of how, when, where and why their private information needs to be used (Das & Teng, 1998). *Within the primary health care facility, it is important that all the co-owners create the perception that they are working together to actively manage the private information of patients whilst administering treatment.*
- **2nd Function of Trust – foster a culture of cooperation**. Establish some norms that guide how decisions are made, so that the choices are perceived to be rational. This assists in reaffirming the credibility and trustworthiness of the trustee (Das & Teng, 1998). *These would be the regulations and best practices that assist patients and co-owners in understanding what they should expect when they interact with or in the primary health care facility.*
- **3rd Function of Trust – reduction in complexity**. By making actions predictable, it is possible to ensure that individuals accept actions as part of a routine (Falcone & Castelfranchi, 2001). *The patient and health care practitioner respond to and act on a situation based on a predefined and understood process, e.g. control mechanisms.*

One can conclude that it is plausible that trust can reduce complexity and uncertainty, which results in a greater level of confidence in a shared relationship. However, trust is not effective unless it is coupled with some form of control (Das & Teng, 1998). Although, trust is associated with the trustor's expectation of action by a trustee, there is no element of influence of the trustor over the trustee. There is the belief that the trustee will act in a certain manner even with the absence of any control, because they can be trusted (Falcone & Castelfranchi, 2001).

Trust allows for the perceived probability of an expected behaviour occurring, whereas control mechanisms provide a means of increasing the probability of that behaviour actually being realised (Das & Teng, 1998). The next section discusses the aspect of

controls within the context of control mechanisms and level of control in order to increase predictability.

3.4. Predictability with Controls

Trust provides a cognitive means to cope with uncertainties that arise from making oneself vulnerable, whereas control leads to the increased predictability of actions through established standards associated with a desired outcome (O'Hara, 2004). Control is associated with two distinct constructs: control mechanisms and level of control (Das & Teng, 1998). Control mechanisms are put in place by an organisation to ensure that members carry out their duties in a given manner (Flowerday & von Solms, 2006). The level of control is an outcome of the control mechanism, in so far as it is possible to determine that the individual will act in a given manner, because of the control mechanism being in place (Das & Teng, 1998). Flowerday and von Solms (2006) indicate that the level of control is determined by the risk appetite of an individual. Subsequently, a control mechanism is expected to provide an optimum level of control over a specific action in order to increase its predictability of occurring in the face of accepted risk (Flowerday & von Solms, 2006). These control mechanisms can be used to ensure that certain activities become routine (Mayer, et al., 1995). They can also be used for non-routine activities, such as awareness programmes that assist in increasing the predictability of future actions (Das & Teng, 1998). Control mechanisms can be divided into those mechanisms that evaluate performance (*formal controls*) and those that deal with the actions of people (*social controls*) (Das & Teng, 1998).

Formal controls are concerned with the establishment of explicit rules and regulations regarding processes to follow and can assist in improving the level of trust in the organisation (Das & Teng, 1998). They provide a means to monitor (audit) the actions of trustees in order to ensure that they are acting in the desired manner. However, it is important that the control mechanism deployed should be suited for the environment, or it may work against it (Mayer, et al., 1995). For example, if the access to patient information is too restrictive, then it may negatively affect the level of

treatment provided to the patient. This may result in the health care practitioner not having access to the patient's medical record. Therefore, formal controls should be concerned with the establishment of clear collective privacy boundaries in order to influence the patterns of behaviour of individuals in a given environment (Petronio & Reierson, 2009). The continued existence of trust is threatened if formal controls are poorly designed (Das & Teng, 1998).

Social control is concerned with the long-term establishment of a trusting relationship by nurturing the organisational culture within the organisation. It can take the form of socialisation, interaction, and training (Das & Teng, 1998). Socialisation and interaction improve understanding and shared values between those in a trusting relationship (Das & Teng, 1998). Training, which follows from increased awareness, can assist in reducing the complexity of the various regulations that need to be followed in the organisation (Whitman & Mattord, 2009). Overall, social controls assist in providing a supportive environment which fosters trust where it may not yet be present, or where it has just formed (Das & Teng, 1998). The establishment of how the health care practitioners process the patient's private information and respond to the environment are of importance to the effectiveness of control mechanisms (Scott, et al., 2007).

Merchant (1984, cited in Das & Teng, 1998) argues that it is inconclusive why the adoption of increasing control mechanisms does not necessarily result in more control. However, for control mechanisms to be implemented there needs to be an initial level of trust (Earle & Siegrist, 2008). If an initial level of trust does not exist then it is not possible to establish mutual goals and establish formal controls to manage processes (Falcone & Castelfranchi, 2001). From the perspective of utility/value, it can be stated that a patient initially has a high level of trust and expects a high return on the amount of risk they are willing to accept. It can be concluded that trust is therefore an initiator and facilitator of control mechanisms (Flowerday & von Solms, 2006; Das & Teng, 1998).

Flowerday and von Solms (2006) depict confidence as a product of trust and controls in

the face of a given risk appetite (*cf.* Figure 3.5). From the perspective of this research project, the risk appetite is the perceived vulnerability associated with the potential loss and exposure of private information to which the trustor is willing to make themselves vulnerable (*cf.* Figure 3.5). The perceived vulnerability (risk) is reflected as E|F, where it reflects a point where trust is sufficient to allow for limited controls to be in place for confidence to exist. Triangle ACD is the trust area and triangle ABD is the controls area. The rectangle ABDC represents the area of information privacy. If we move E|F closer to A|C, then we are heading towards a point of absolute trust, where the reliance on controls is reduced. A state of absolute trust can be assumed to not exist in the health care sector, because the Hippocratic Oath exists to guide initial interaction of the patient and the health care practitioner. Therefore, there is no blind trust in the health care practitioners, but rather private information is shared given the perception of the patient that some form of controls exist to protect their private information.

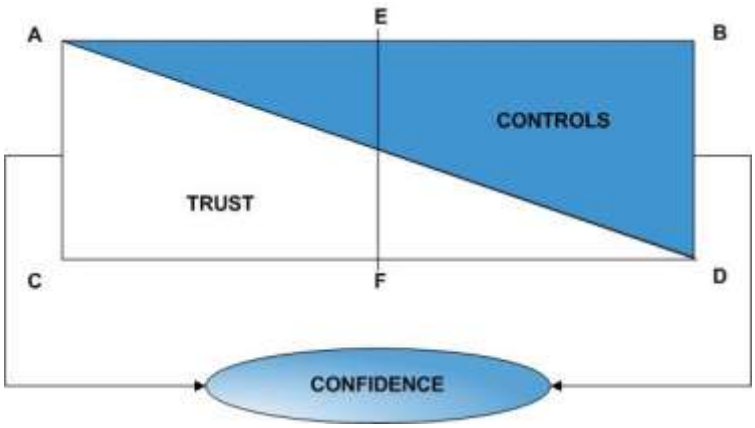


Figure 3.5: Relationship between trust, controls and confidence (Flowerday & von Solms, 2006)

If we move E|F in the opposite direction towards B|D, then we are heading towards a point of rigid formal controls, or absolute controls. A state of absolute controls would mean that the existence of trust is not necessary in order to gain confidence, which is contrary to the need in the health care sector.

If we consider the three zones mentioned earlier in the chapter (*cf.* Section 3.2), then we can further deduce that as the private information of the patient moves through

the zones it correlates with a steady movement of E|F towards B|D. The changes to the level of trust and controls utilised is impacted by the dynamic nature of trust. Therefore, control mechanisms used will differ in varying degrees of formal and social control in response to changes in trust, so that a violation of confidentiality can be avoided.

3.5. Violation of Confidentiality

A violation of confidentiality occurs when the original expectation of the trustor with respect to how their private information would be managed is compromised (Falcone & Castelfranchi, 2001). When confidentiality is violated, it threatens to disrupt the relationship that was originally based on a given level of trust about how the private information would be managed (Deshefy-Longhi, et al., 2004). Petronio and Reierson (2009) state that the collective privacy boundary enters a state of boundary turbulence, where there is a chance the boundary might no longer be viable.

Within the context of CPM theory, Petronio and Reierson (2009) provide three categories for explaining breaches in confidentiality associated with privacy, namely:

- ***discrepancy breaches of privacy*** – the expectation of the trustor about how the trustee will manage their confidential information does not mimic practice when dealing with 3rd parties, and those who become intentional or unintentional co-owners of the information. *For example, a patient receives blood test results from an employee at a medical laboratory instead of from her doctor. The patient had expected the doctor to contact her.*
- ***privacy ownership violation*** – a trustor's ability to exercise control and ownership is violated when their beliefs with respect to the regulation of their private information are compromised. *For example, the patient feels that they did not give consent for their medical information to be shared and now question who has access to the information.*

- ***pre-emptive privacy control*** – a trustor having experienced a previous privacy breach or uncertainties with respect to levels of trust is hesitant to enter confidential relationships for fear of a breach. These individuals will require controls that establish thick boundaries in order to prevent disclosures or/and require explicit permission for access to their private information.

The types of breaches mentioned above relate mostly to the patient's (trustor's) understanding of a violation of confidentiality. However, it should be noted that a discussion on a loss of confidentiality encompasses not only the patient-health care practitioner dynamic, but all those who have access to the private patient information, i.e. all trustees within the collective privacy boundary. Williams (2008) investigated primary health care facilities and determined that there is a serious disregard for acknowledging security threats. She identified four areas of concern, namely:

- ***lack of sensitivity to private information*** – health care practitioners believe that the freedom to share confidential information during a patient's treatment far outweighs any concerns for their information privacy. There is a lack of understanding as to why information privacy is of importance.
- ***lack of conceptual understanding of information security*** – there is a lack of awareness of the information security concerns when dealing with confidential information and the legal ramifications should there be a violation of the confidential information.
- ***underestimation of threats*** – the reason for the underestimation has been attributed to both awareness and cultural factors. Most primary health care facilities are concerned with improving patient treatment and administration processes, and often overlook security issues.
- ***technology meets culture*** – the use of technology in the health care domain is not uncommon, but the majority of breaches still tend to be attributed to humans disclosing information. Technology may provide greater controls, but it also makes information more accessible

especially in the health care context where multiple individuals access confidential information.

The utilisation of control mechanisms, especially social controls, given the concerns above could potentially result in a better understanding of the workflow processes associated with confidential information. Whitman and Mattord (2009) suggest that confidential information can be protected through information classification (i.e. only those with certain roles can access it), secure document storage, security policies, and educating data subjects and data controllers about managing the information. These aspects are extrapolated further in Chapter Four.

Improving an understanding of the processes associated with the development, control, and violation of confidentiality assists in navigating the dynamics of confidentiality regulations (Petronio & Reierson, 2009). The next section considers the regulation of confidentiality by reviewing the Caldicott principles (Keyser & Dainty, 2005) and the Health Professions Council of South Africa guidelines relating to confidentiality (HPCSA, 2007).

3.6. Regulating Confidentiality

Legal remedies do not always engender trust (Solove, 2008). However, they are required in order to effectively establish controls that manage confidentiality (Huang & Fox, 2006). The next section will discuss the Caldicott principles.

3.6.1. Caldicott Principles

The Caldicott Principles[14] for dealing with confidentiality arose from a review of the information management practices for protecting patient information by the National Health Service (NHS) in the UK (Keyser & Dainty, 2005). These principles

[14] The commission was headed by Dame Fiona Caldicott and the principles were named after her (Keyser & Dainty, 2005).

operationalised within the UK health care sector were based on the Data Protection Act (1998) which was passed in the UK, and in turn originated from the European Commission (EC) Data Protection Directive (Directive 95/46/EC) (Keyser & Dainty, 2005). The Act provided eight data protection principles, which sought to establish standards on how personal data could be obtained, recorded, stored, used or disposed of. The UK Data Protection principles are listed in Table 3.1.

The Caldicott Principles in turn provide a means to control the private information of the patient as it moves through the three zones of information dissemination (*cf.* Section 3.2). Table 3.2 lists the six Caldicott Principles and provides a brief description of how each is relevant within the primary health care facility.

Table 3.1: Summary of the UK Data Protection Act of 1998 (Keyser & Dainty, 2005, pp. 96-101)

#	UK Data Protection Act Principle	Description
1	Personal data should be processed in a fair and lawful manner.	The data controller (health care practitioner) needs to inform the data subject (patient), without subterfuge, about the processing of their private data, so that there is no doubt as to: - why their data is being collected; - what it is going to be used for; - who it may be shared with; and, - at all times the data subject must have a choice as to how their data is handled.
2	Personal data should be processed for an intended purpose.	There is greater transparency for the data subject as to how their data is being processed and places restrictions on what the data controller can process the data for in the future. Confidential data collected cannot be reused for another purpose if there has been no consent.
3	Personal data should be collected that is adequate, relevant and not excessive for the intended purpose.	The use to which data is to be applied must be known to the data subject and the data handler, so that no irrelevant data is collected.
- continued on next page-		

Table 3.1 (continues)		
4	Personal data should be accurate and kept up-to-date.	The data controller needs to ensure that the data received from the data subject has been supplied correctly and must make any changes identified by the data subject.
5	Personal data should not be kept longer than necessary.	The various legislative rules with respect to the retention of records need to be adhered to by the data controller.
6	Personal data should be processed in accordance with the rights of data subjects.	The data subject's privacy rights should guide how their data is managed. Where a medical decision is to be made solely by a decision support system, the data subject should be informed.
7	Personal data should be protected by appropriate security *(both practical and organisational)*.	The data controller is responsible for creating and adhering to information security measures.
8	Personal data should not be transferred beyond the boundaries of the European Economic Area (EEA) without adequate protection.	This principle falls outside the direct scope of the data subject/controller relationship, but the onus falls on the data controller to ensure that electronic medical information is not transferred without the consent of the data controller and within existing laws.

Table 3.2: Caldicott Principles for health care confidentiality (Keyser & Dainty, 2005, p. 8)

#	Caldicott Principle	Description
1	Justify the purpose	Any proposed use or transfer of patient PII within or from the primary health care facility should be clearly defined, scrutinised and future uses reviewed.
2	Do not use patient PII unless it is absolutely necessary	Patient PII (*cf.* section 2.4.1 above) should only be used if there is no alternative course of action. As far as possible, the anonymity of the patient should be ensured in the primary health care facility.
3	Use the minimum necessary patient PII	The use of any PII should be justified on the basis that the care could not be provided if it was not present.
4	Access to patient PII should be on a need-to-know basis	Only those authorised individuals who need a specific piece of patient PII should have access to it, but they should not have access to any other PII.
5	Everyone should be aware of his/her responsibilities	Action should be taken so that clinical and non-clinical staff becomes aware of their responsibilities and obligations to respect patient confidentiality.
6	Understand and comply with the law	Every use of patient PII must be lawful and there should be a data controller responsible for ensuring that the law is followed.

The Caldicott Principles were reviewed as they related directly to the discussion of privacy addressed in Chapter Two. They provide a concise overview of the obligations of the health care practitioner in a primary health care facility in the UK. It is not impractical to consider that these same principles could be applied to the South African health care sector.

Subsequently, it is also prudent to review the relevant confidentiality guidelines associated with health care in South Africa to see if they are indeed similar to the Caldicott Principles. The next section addresses this issue.

3.6.2. Health Professions Council of S.A. (HPCSA) Guidelines for Confidentiality

The South African legislation associated with confidentiality and health care, includes, but is not limited to the: Child Care Act; Aged Persons Act; Medical Scheme Act; and, the National Health Act. The HPCSA provides guidelines for good practice in the health care professions. Booklet 11 provides guidelines on confidentiality with respect to the protecting and providing of information (HPCSA, 2007). The guidelines are based on international ethical codes[15], the South African Constitution (Act No. 108 of 1996) and the National Health Act (Act No. 61 of 2003).

According to the National Health Act, all patients have a right to confidentiality, which is consistent with the right to privacy in the SA Constitution (HPCSA, 2007). The confidentiality guidelines provided by the HPCSA are extensive and consequently they have been summarised in Table 3.3 in order to facilitate the discussion of this research project.

[15] The World Medical Association (WMA) International Code of Ethics states: "A physician shall preserve absolute confidentiality on all he knows about his patient even after the patient has died." Although, most ethical codes now make exceptions for legal requirements, to protect those that could be harmed by not divulging information and disclosure to other health care workers in the interest of the patients.

Table 3.3: Summary of the HPCSA Confidentiality Guidelines (HPCSA, 2007)

#	Confidentiality Guidelines	Description
1	Retention of Confidentiality	Health care professionals[16] must justify their decisions with respect to providing information about patients by seeking patient consent, anonymising the patient's PII, and minimising disclosures.
2	Protection of Information	Health care personnel[17] need to be made aware of the necessary processes for securing patient PII against unintentional disclosures of the patient's PII.
3	Right to Information	Patients have the right to be kept informed about the information that is needed for their current treatment and future treatment options.
4	Disclosure of information	Patients must provide consent (explicit or implied) in order for their information to be disclosed to health care personnel. All recipients must ensure that they hold the information received in confidence even if they are not directly involved in the treatment of the patient.
5	Securing electronic information	Health care practitioners must make the necessary information security arrangements to secure personal information when it is stored, sent, or received electronically.
6	Accountability to the public and the law	Health care practitioners are responsible for their actions and should they not follow the guidelines as stipulated, then they need to justify their actions to the public they serve, regulatory bodies (HPCSA), and the law.

The Caldicott Principles and the HPCSA Confidentiality Guidelines have a number of similar requirements for how confidentiality should be managed, as they are both based on the FIPs (*cf*. section 2.5 above) and the idea of patient control. However, Woodward (2001) states that there is an ongoing debate between disclosure and consent with respect to a patient's medical records. The FIPs are fundamentally concerned with the disclosure of private information, whereas concerns of confidentiality and consent are associated with the control of the patient over their records (Nissenbaum, 2010). Furthermore, the extensive dissemination of EMRs makes it increasingly difficult to seek permissions from the initial patient to access and share their medical data at multiple instances (Deshefy-Longhi, et al., 2004). This

[16] For the purposes of these guidelines, the term 'health care professionals refers to practitioners registered with the HPCSA (HPCSA, 2007).

[17] 'Health care personnel' in terms of the National Health Act includes both health care providers and health workers (i.e. the health care team that provide clinical services for patients, and the administrative staff who support these services). The Act includes health care professionals under the term 'health care providers' (HPCSA, 2007).

makes complete control on the part of the patient over their medical records difficult in practice (Tavani, 2008).

Woodward (2001) states that the traditional view of the doctor-patient relationship has changed from a largely private relationship to a health care sector relationship, where patients are pawns at the mercy of institutional behemoths (e.g. medical aids). The extent of the data collection and dissemination makes it appear impractical to even consider consent (Woodward, 2001). However, confidentiality cannot exist in the absence of consent, because it effectively means that the collective privacy boundary once established is immediately porous (Petronio & Reierson, 2009). Therefore, it is necessary that patients are informed about the extent of the confidentiality being offered and the limitations of how the information will be managed (Whitley, 2009; Petronio & Reierson, 2009). Restrictions with respect to release without consent are increasingly included in laws and regulations which often include punitive recourse if information is released without consent (Appari & Johnson, 2010; Grandison & Bhatti, 2010; Woodward & Hammerschmidt, 2003). Additionally, they include standards to be followed for making private information anonymous to protect patients when consent cannot be obtained, or disclosure is unavoidable (ISO/IEC 29100, 2011; Narayanan & Shmatikov, 2010; ISO/IEC 27799, 2008).

Although laws and regulations exist, it is largely up to individual primary health care facilities as to how these will be operationalised (Gerntholtz, van Heerden & Vine, 2007; Woodward, 2001). These facilities, when determining how to make private information available and yet still protect it, will decide on a mixture of formal and social controls to maintain the collective privacy boundary. The establishment of social controls will assist in making health care workers aware of the significant impact that they have on the information privacy of patients.

3.7. Conclusion

This chapter considered the notion of confidentiality and how individuals need to determine how relationships are established. Confidentiality is the cornerstone of

medical practice and therefore the establishment of the relationship between the patient and the health care practitioner was discussed. It was found that patients will typically establish relationships based on trusting relationships where the trustor (patient) determines the level of trustworthiness of the trustee (health care practitioner). By determining the level of trust, it was found that controls needed to be considered as a means to add confidence to the confidential relationship that was created. The right mix of trust versus control would therefore give rise to increased predictability in the relationship. Controls were discussed as playing a significant role when the patient's EMRs are shared with those in other zones of care, other than the zone of primary care.

However, given the number of individuals who have access to the patient's medical data throughout the treatment process, it was realised that violations of confidentiality are likely to occur. The existence of legal recourse and guiding principles, such as the South African Health Professionals guidelines of how confidentiality should be maintained by those employed at a primary health care facility were discussed at the end of the chapter.

From a theoretical perspective, Principle 2 of the CPM Theory was considered and built on Principle 1 dealt with in Chapter Two. The factors that determine the rules an individual applies to establishing their privacy rules for concealing and revealing was evidenced by the choice to trust another individual. Principle 3 of the CPM Theory expanded the issue of confidentiality, where the trustor makes a decision to trust the trustee thereby creating a confidant and co-owner of the private information.

The principle associated with Control Theory was considered with respect to the individual's choice to share their private information and their ability to control who had access to their private information. Fundamental to this is the control that the individual exercises over the relationships that they create.

Principle 4 of the CPM Theory, which deals with negotiating how those in a confidential relationship will share private information with others, was implied in this

chapter. However, the granting or denying of access through consent to private information is both relevant to the confidential relationship and the accessibility to private information, so will also be considered in Chapter Four.

The next chapter considers how information concerning a patient is made accessible at a primary health care facility, so that patients receive the treatment required. The discussion will be framed within the context of socio-technical systems and explored with reference to the concern for information privacy (CFIP).

CHAPTER FOUR: ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

CHAPTER ONE:
INTRODUCTION

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

- 4.1. Introduction
- 4.2. Concern for Information Privacy (CFIP)
- 4.3. The Socio-Technical Theory
- 4.4. Technical and Environmental Perspective of Health Care
  - 4.4.1. Benefits of Adopting Electronic Medical Records (EMRs)
- 4.5. Social Perspective of Health Care
  - 4.5.1. Collecting Patient Information
  - 4.5.2. Errors in Patient Information
  - 4.5.3. Unauthorised Access to Patient Information
- 4.6. Cultivating a Security Culture
- 4.7 Conclusion

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

4.1. Introduction

In Chapter Two, the concept of ***privacy*** ownership was discussed with respect to the various privacy constructs and the arising legislation. The discussion was framed by considering two theories, namely: Communication Privacy Management (CPM) Theory and Restricted Access Theory. The CPM Theory is referred to throughout this research project and considers the changes in privacy boundaries that occur as an individual moves from a state of complete ownership to the sharing of the private information with co-owners (Petronio & Reierson, 2009). In Chapter Two, the focus was on *Principle 1* of the CPM Theory, which involves the ownership and control of private information (Petronio, 2002). The Restricted Access Theory addresses the issue of limiting or restricting access to one's private information (Tavani, 2008).

In Chapter Three, the concept of ***confidentiality*** and trust was discussed and specific to this discussion was the issue of control. The CPM Theory was expanded into this chapter's discussion by considering *Principle 2*, which considers the rules for concealing and revealing, and *Principle 3*, where disclosure creates a confidant and co-owner (Petronio & Reierson, 2009). The principle associated with Control Theory was considered with respect to the individual's choice to share information (Tavani, 2008). It focused on the individual's ability to control who had access to their private information and their control over the creation of relationships (Tavani, 2008).

This chapter investigates the various factors associated with making EMRs ***accessible*** for use. This includes a discussion of what is required for records to be available and also ensuring their integrity. Availability within the context of this research project is concerned with making EMRs accessible and usable when they are required by authorised health care personnel or a given information system (Appari & Johnson, 2010). Integrity is concerned with the safeguarding of the accuracy of records to ensure that they are complete and error free (Whitman & Mattord, 2009). Within the health care sector, poor integrity of a medical record could literally mean the difference between life and death (Agrawal & Johnson, 2007). Ironically, errors by employees are a significant threat to any organisation (Whitman & Mattord, 2009).

The use of the CPM Theory to facilitate the discussion is concluded in this chapter by investigating the issues surrounding *Principle 4*, which is the coordination of mutual privacy boundaries and the notion of consent, and *Principle 5*, which looks at boundary turbulence, or factors that can affect accessibility (Petronio & Reierson, 2009). Furthermore, the concept behind the Restricted Access / Limited Control (RALC) Theory is considered, that is a hybrid of the Restricted Access and Control Theories (Tavani, 2008). In the RALC Theory, the notion of restricted access is associated with the concept of privacy, and the management of privacy with a system of limited controls (Tavani, 2008).

This chapter explains the constructs behind the final principles of the CPM Theory and the RALC Theory by firstly reviewing the concerns for information privacy (CFIP) and then applying these within the framework of Socio-Technical Theory. The discussion is focused within the context of health care. The benefits that can arise from the adoption of EMR are briefly explored. The research project expands on the CFIP associated with collecting patient information, errors in patient information, and authorised access to patient information. Throughout the notions of control and consent, which are associated with the CPM Theory and RALC Theory, are discussed. Finally, the chapter concludes with a brief discussion of how a security culture may be cultivated, so that a greater awareness of information privacy can be fostered. This leads to the ultimate goal of this research project, which is to provide an informational privacy model, which can improve the awareness of health care personnel of privacy legislation.

4.2. Concern for Information Privacy (CFIP)

Smith, et al. (1996) proposed the CFIP as a construct that seeks to measure an individual's attitudes and beliefs when confronted with how another's private information would be used. The CFIP is comprised of four factors, namely: collection, errors, unauthorised access, and secondary use (Smith, et al., 1996; Angst & Agarwal, 2009). Furthermore, the CFIP can be logically associated with the principles of fair

information practice (FIP)[18], which have guided much of the privacy discussion since the 1970s (*cf.* Section 2.6). The CFIP are described as follows (Smith, et al., 1996):

- ***Collection*** can be described in terms of the growing trend to collect vast amounts of personally identifiable information (PII) in the pursuit of an alternative purpose, rather than finding ways to reduce that which is collected **[Choice/Consent]**.
- ***Errors*** can arise when capturing and processing PII and procedures need to exist that minimise errors by assigning responsibility for their identification to individuals or an information system **[Integrity/ Security]**.
- ***Unauthorised access*** is associated with determining how controls are applied and administered with respect to restricting access to PII to authorised individuals **[Access/Participation]**.
- ***Secondary use*** is concerned with using or sharing PII without authorisation for a purpose other than that for which it was intended when it was collected **[Enforcement/Redress]**.

The descriptions of the factors are on the face of it evident (visible), but also allude to the covertness associated with information privacy. The paradox of information privacy being both visible and yet also hidden when associated with the CFIP, arises out of the effect the factors have to consciously and unconsciously change the attitudes of individuals to follow a set course of actions within a given context (Angst & Agarwal, 2009). The popular analogy of what lies beneath the surface of an iceberg is indicative of the myriad of influences that determine how an individual would react to a given concern associated with information privacy. From earlier discussions (*cf.* Chapter Three) on confidentiality and trust, it is evident that individuals are not likely to create collective boundaries unless they are confident of an expectant outcome. The choices made with respect to trust and confidence do inherently come with

[18] The relevant FIP that can be associated with the CFIP is shown in square brackets at the end of description of each CFIP.

concerns, but these are considered to be offset by the existence of controls and legislative protection remedies (Falcone & Castelfranchi, 2001).

Smith, et al. (1996) further identified two ancillary issues, which were associated with the influence of technology on the four concerns, namely: the *reduction in human judgement* by increasing the reliance on automated decision making; and, the *assimilation of data* which seeks to use technology to create a singular collective view of an individual's data. Within the health care context these would apply to a reliance on automated systems to make diagnostic decisions in the absence of a human (Angst & Agarwal, 2009), and profiling individuals through the data collected, such that confidentiality is no longer in evidence (Appari & Johnson, 2010). It is therefore, not unreasonable to assume that technology can on the one hand be an enabler to the health care profession, but on the other an inhibitor if individuals perceive they will experience a loss of control. Interestingly, O'Hara (2004) clarifies the paradox that arises from trust associated with humans and technology by stating technology can and will fail at some point, but it is less likely to be the culprit. According to Ciampa (2010), that honour belongs to humans. This revelation leads to the need for individuals to be increasingly made aware of the various social factors associated with using given technologies, so that the instances of misappropriate use or failure are reduced (Herold, 2011).

However, prior to exploring the CFIP raised in this section it is necessary to consider how to bring the various social and technical concerns into harmony. If one views health care from a socio-technical perspective, then harmony has to exist between the technical and social systems, which seek to provide care for the patient, but at the same time protect their information privacy. The next section briefly introduces the main constructs of the Socio-Technical Theory, which will be used to frame the discussion for the remainder of the chapter.

4.3. The Socio-Technical Theory

By utilising the main constructs of the socio-technical theory, it is possible to explain health care as a multi-faceted functioning system (Whetton, 2005; Li, 2010). If one considers the theory in terms of the impacts of Information Technology on the primary health care facility *(organisation)*, it is possible to identify the technical *(i.e. the devices and tools used to capture, process and output information)* and social *(i.e. the employees, their value systems, and authority structures)* sub-systems in existence. The technical sub-systems are concerned with how the processing of ***tasks*** can be done more effectively and efficiently by utilising given ***technology***, e.g. when moving from paper-based to electronic medical records. The social sub-systems focus on the ***people*** (i.e. health care personnel) interacting with the various technologies to complete their required tasks within the ***structures*** (i.e. rules and regulations) of the organisation, e.g. when health care personnel access a patient's EMR provided they have the appropriate authorisation. The two systems are independent and yet reliant on each other in order to produce the desired outcomes from their interactions (Li, 2010).

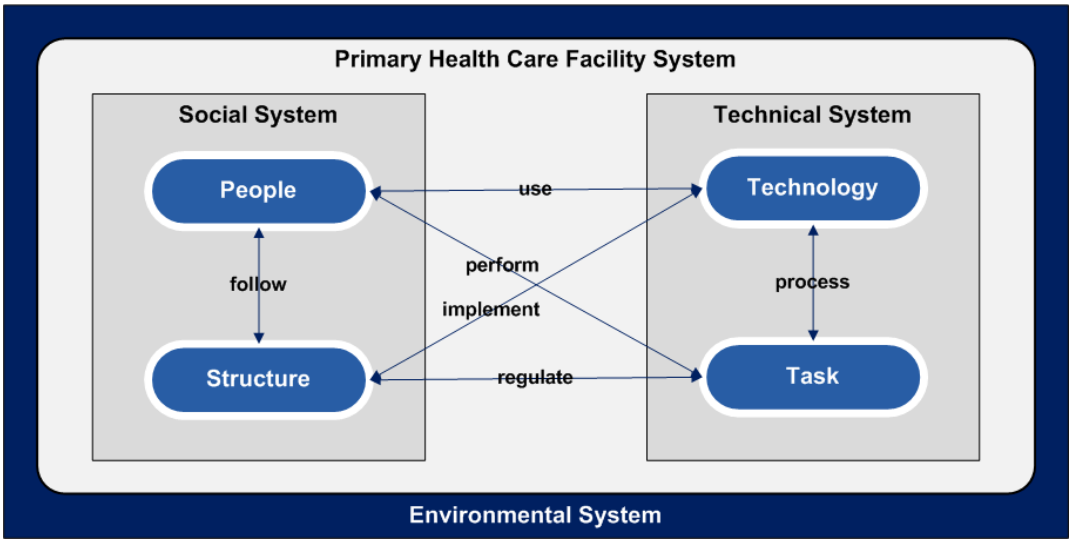


Figure 4.1: Socio-Technical Primary Health Care Facility System (adapted from Bostrom & Heinen, 1977)

Figure 4.1 reflects the interacting variables associated with the various working sub-systems. The bi-directional flows of information between the work sub-systems at a

primary health care facility have been labelled in order to provide a narrative to reflect the interactions. These can be explained as follows:

- **People** *(e.g. health care personnel)* make use of a given **technology** *(e.g. devices and tools)*, and **technology** is used by **people** to carry out their work.
- **People** perform a given **task** (e.g. record medical data), and a **task** is performed by **people**.
- **People** follow a given **structure** (e.g. set of rules), and a given **structure** is followed by **people**.
- **Structure** regulates how a **task** should be completed, and a **task** is regulated by **structure**.
- **Structure** guides the implementation of **technology**, and **technology** is implemented because of required **structure**.
- **Technology** will process a **task**, and a **task** will be processed by **technology**.

Whetton (2005) states that an additional system was later proposed in terms of socio-technical theory, namely: an environmental system. From the perspective of this research project, this system is external to the primary health care facility. It includes such entities as the patient, medical aids, and legal compliance requirements, which prescribe what controls need to be in place in a given facility (Li, 2010). The distinction between the primary health care system and the environmental system can be clearly linked to the earlier discussion on the zones of care (*cf.* Figure 3.1, where zone 2 and 3 are the environmental system) and to Figure 4.2 in the next section.

The earlier discussion of contextual integrity (*cf.* Section 2.2) further highlighted the need to take consideration of the individual privacy rights associated with a given context, as the interpretation of the right to privacy differs from setting to setting. Therefore, it is necessary to be mindful of the context, informational norms, actors/roles, attributes and transmission principles that have to be present to avoid an infringement on informational privacy (Nissenbaum, 2010).

The next section will briefly discuss the technical and environmental perspectives associated with the health care sector. The section following it will then focus on the social perspective as it relates to the impact that the primary health care facility and health care personnel have on the delivery of medical care. The patient will be an important part of the discussion to follow and for the sake of clarity; it is assumed from this point in the research project that the patient only becomes a member of the environmental system after they have completed their initial consultation with the primary health care facility.

4.4. Technical and Environmental Perspective of Health Care

Carr (2004) in his seminal work on the strategic importance of information technology (IT) argued that IT is no longer a competitive advantage, but rather a required input (i.e. cost of doing business) to be experienced by all parties. He further states that "the fragmented health care industry [see Figure 4.2[19]], shielded from competition, has been relatively slow to adopt IT, despite its complex information and transaction processing requirements" (Carr, 2004, p. 67).

This is in part due to an erroneous view by the pundits of increased IT adoption in health care, that IT could simply be slotted into the sector and would be enthusiastically accepted by all users (Whetton, 2005). However, there is reluctance by health care providers to adopt integrated IT based in part on concerns of IT costs, cultural factors and information security (Appari & Johnson, 2010). Yet health care legislation and financial assistance (being provided in various parts of the world, e.g. HIPAA/HITECH in the United States) make the adoption of EMRs increasingly more favourable (Grandison & Bhatti, 2010). The cultural factors arise from the willingness of potential or current users of EMR systems to accept that it is necessary to change

[19] Figure 4.2 can be generalised to the SA health care sector if we omit: Medicare (under Payers), which is a public health grant paying system – similar to the NHS in the UK, and the proposed National Health Insurance for South Africa. Health Bank refers to online electronic health records. Some payers, such as Discovery Health are rolling out these options to their members in South Africa.

the way that they interact and manage the medical records of their patients. Often once the process has been refined, many find the electronic medical record system is indispensible in the operations of their facility (Gerntholtz, et al., 2007). However, as increasing amounts of information are gathered electronically and shared through the various interconnected entities, information security concerns increase and confidentiality becomes increasingly difficult to maintain (Agrawal & Johnson, 2007).

The information security concerns are not insurmountable and there are numerous control mechanisms to provide for formal controls to assist in reducing the likelihood of an information security incident occurring (Angst & Agarwal, 2009). However, it is necessary that health care personnel and patients are kept aware of the various proactive and reactive means to ensure that there is no intentional or accidental breach in information privacy.

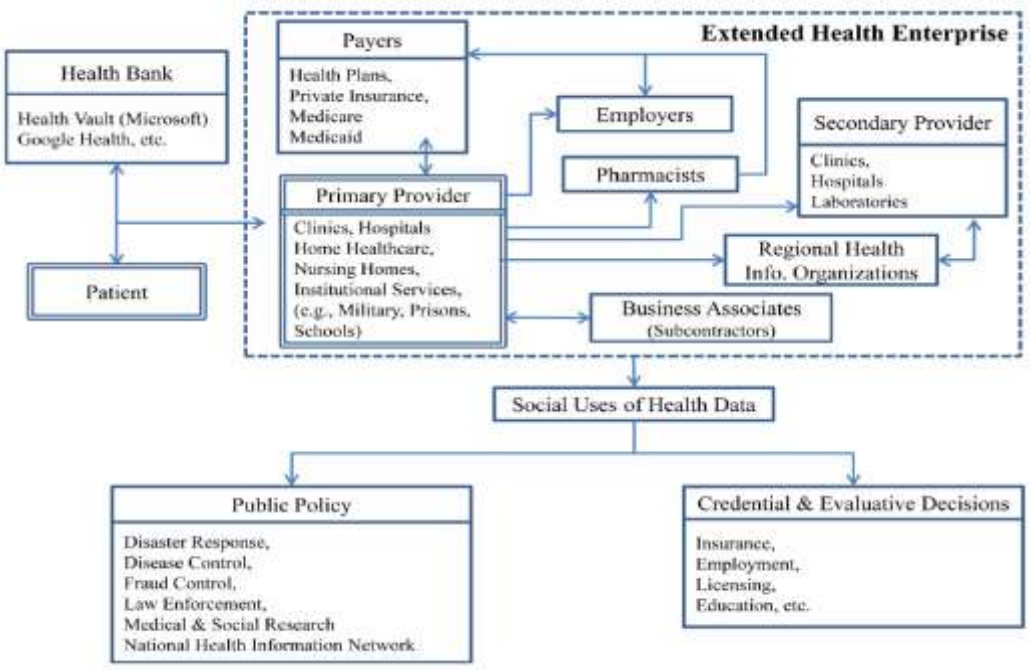


Figure 4.2: Informational flows in the health care sector[20] (Appari & Johnson, 2010)

[20] da Veiga and Hari (2011, p. 44) provide a similar diagram to Figure 4.2 of the health care sector in South Africa. However, their focus is to indicate the responsible parties for carrying out the principles as detailed in the Protection of Personal Information (PoPI) legislation, so lacks the details shown here.

Therefore, an understanding of the application of social controls associated with organisational and cultural factors are needed (Whetton, 2005). This is to ensure that it is possible to raise awareness of the issues associated with respect to the protection of PII in an EMR while it is in motion and at rest, because this is a critical aspect of information security (Whitman & Mattord, 2009). However, prior to considering the social perspectives of health care associated with the interaction of the people, structures, tasks and technology, it is necessary to consider what the actual benefits might be of adopting electronic medical records.

4.4.1. Benefits of Adopting EMRs

Terry and Francis (2007) define an EMR as located within the offices of a single primary health care provider and containing a patient's history of care. When a patient's record stretches across multiple providers and in some instances is accessible directly by the patient, they are known as electronic health records (EHR) (Angst & Agarwal, 2009; Agrawal & Johnson, 2007). The focus of this research project is on the EMRs being managed at a primary health care facility.

The overriding issue surrounding medical records, whether paper-based or electronic, centres on the issue of maintaining the patient's privacy by ensuring that PII is kept confidential, but yet also made available (ISO/IEC 27799, 2008; Goodman, 2008; Lederman, 2005). The benefit of adopting EMRs arises from an anticipated improvement in the care of the patient, because of the increased accessibility of the patient information (Goodman, 2008; Gerntholtz, et al., 2007).

Terry and Francis (2007, p. 682) identify several advantages that can be realised from the adoption of EMR, namely:

- ***Legible records***, that are easier to read than a paper-based record as there is no need to attempt to decipher a doctor's handwriting.

- ***Searchable records***, that a health care provider can use to identify any conflicts that may arise in following a given treatment, or to formulate a previously unknown diagnosis.
- ***Evidence-based protocols***, which allow the symptoms of patients to be automatically, matched against previously unknown treatment plans.
- ***Interconnected records***, that avoid the problems caused by departmental silos of patient information by providing a holistic view of the patient care needs.
- ***Accessible records***, where authorised health care personnel can access the patient record from any computing device, rather than accessing the file in a central location.

Therefore, EMRs can make it easier to compile, store, retrieve, manipulate, and audit the movement of a patient's PII throughout the primary health care facility (Scott, et al., 2007; Gerntholtz, et al., 2007). Unfortunately, the increased accessibility of EMRs is paradoxical, as it provides at the same time immense benefits, but also leads to increasing concerns of the ease of unauthorised access (Angst & Agarwal, 2009). Furthermore, the dissemination of a single paper-based record is limited, but an EMR can be replicated at alarming speed (Agrawal & Johnson, 2007). This leads to concerns about privacy and confidentiality associated with PII becoming public (Smith, et al., 2011; Whiddett, et al., 2006).

The next section will focus on discussing three of the four concerns for information privacy, namely: collection, errors, and unauthorised access. The concern with information being utilised for secondary use will be mentioned only briefly when discussing the other three. The discussion will be done within the context of the social system of the socio-technical theory, i.e. the focus will be primarily on the sub-systems of people and structure. Although, it is not possible to completely separate them from the sub-systems of technology and task, as the systems are interdependent.

4.5. Social Perspective of Health Care

Prior to discussing the various social issues that arise with respect to information privacy, it is necessary to revisit why information privacy is becoming an increasing issue with the use of information and communication technologies (ICT). Tavani (2008) identifies four information privacy factors that need further analysis, namely:

1. The amount of personal information that can be collected.
2. The speed at which personal information can be exchanged.
3. The duration the information can be retained.
4. The kind of information that can be acquired.

Factors 1, 2, and 3, link directly to the CFIP and the effect of an increase in the quantity of information being collected (Tavani, 2008). Factor 4 is concerned with an increase in the quality of information that is collected and who should have access to the information (Tavani, 2008). These various aspects will be woven throughout the discussion in the sub-sections to follow in order to answer various concerns that patients and health care personnel may have with respect to the information privacy.

Whiddett, et al. (2006) found from research conducted at primary care facilities in New Zealand that patients wanted health care providers to keep them informed about how their PII would be shared. More specifically, they wanted to know:

- Who would be receiving their information other than the health care practitioner?
- What controls there were in place to allow them to share information anonymously?
- How much private information was required?
- What their information will be used for, and who was the intended recipient(s)?

- If they would be consulted prior to the distribution of their information?

Those working at the primary health care facility need to be able to provide information to patients on the above questions in order to increase the patient's perceived trust that their PII will be protected (Whiddett, et al., 2006). The questions provided above are addressed in the general discussion within the next three sub-sections by considering the issues surrounding the collection of patient information, errors in patient information, and the unauthorised access to patient information.

4.5.1. Collecting Patient Information

Whitman and Mattord (2009) stated that information only has value if it can be used for some specific purpose. However, if information is available, but not in a useful format then it is useless (Whitman & Mattord, 2009). This sentiment was also mentioned in Chapter Two when the concept of information was being introduced (*cf.* Section 2.4). Similarly, if a patient decides to withhold certain information from the health care practitioner, because they do not trust that their private information will be secure, then the incomplete information provided may lead to an incorrect diagnosis (Petronio & Reierson, 2009).

In order to be treated patients need to provide some form of consent to a health care practitioner (Keyser & Dainty, 2005; Woodward, 2001). However, the effectiveness of the consent is largely dependent on the choices that were offered to the patient by the health care practitioner (Woodward, 2001). Furthermore, even if consent has been applied, the co-owners of the patient's information can sometimes forfeit a patient's interests, if they misinterpret it as competing against a public interest (Petronio & Reierson, 2009; Nissenbaum, 2010); for example, if withholding information about an illness based on the patient's choice of consent could harm others (Petronio & Reierson, 2009).

Coiera and Clarke (2004, cited in Whiddett, et al., 2006) identify four terms of consent that can be found, namely:

- ***General consent***, where a patient waivers complete control over how their information will be shared. This is similar to the concept of opt-in, where in this case it would be the default.
- ***General consent with specific denial***, where the patient provides limited control with restricted access on how their information will be shared.
- ***General denial with specific consent***, where the patient restricts access, but allows limited control on how their information will be shared.
- ***General denial***, where there is a complete restriction of access, which will require a patient to consent for each and every procedure before it is performed. This is similar to the concept of opt-out, where in this case it would be the default.

Whiddett, et al. (2006) propose that of the four types of consent provided, *general consent with specific denial* would be the best option for the primary health care facility, as it restricts the information the patient believes is too sensitive. Lederman (2005) warns that patients must be mindful of the type of consent they are providing, because providing *general consent* prior to treatment, means the patient has no idea what information will be collected and shared. Additionally, opting for *general denial* might have severe medical repercussions for the patient, because when information is needed it is inaccessible (Lederman, 2005). Terry and Francis (2007) caution that those patients that decide to opt-out should be protected under legislation from discrimination.

The various options for consent mentioned above could function electronically where the system uses electronic consent to determine the authorisation to access certain sensitive patient information. This approach is expected to raise the patient's level of trust, so that they feel more confident that their PII will be kept secure (Padayachee &

Eloff, 2006). An example, of how this type of system might operate is depicted in Figure 4.3. The figure will not be explained further, other than to say that it is an automated consent system where patients authorise what they want to restrict access to, so that consent is more structured for the patients and health care personnel.

Terry and Francis (2007) explain the premise behind Figure 4.3 as applying 'data carve outs'. These are control mechanisms that allow the patient to lock certain parts of their EMR/EHR, which can only be accessed with their consent.

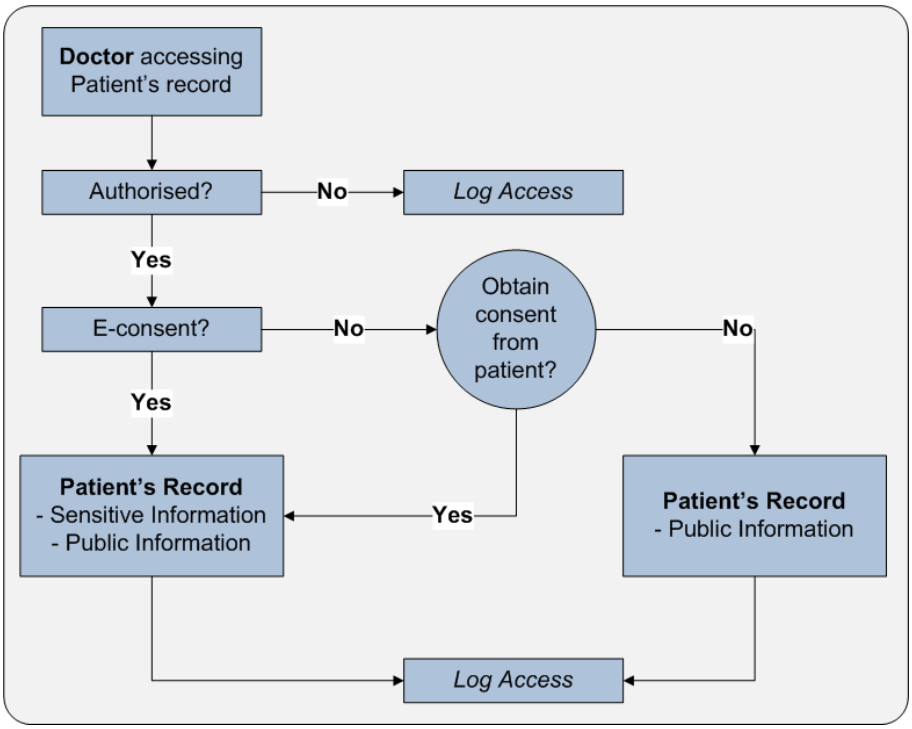


Figure 4.3: E-consent as part of the authorisation process (Padayachee & Eloff, 2006)

The three methods they can use are:

- ***Secure 'envelope'*** – patients opt-in, but certain items are tagged as "highly confidential". The 'envelope' is opened by the patient, or automatically opens if a pre-set condition is met. The nature of the contents of the 'envelope' is not known to anyone other than the patient.

- ***Contextual disclosure*** – patients (in consultation with the health care practitioner) create different 'layers' of visibility that can only be accessed by specific health care personnel.
- ***Access & edit*** – if the patient is permitted access directly to the record, then he can make changes to the existing record by moving certain information to folders where it is once again restricted from access. This should be carried out in consultation with the health care practitioner.

Woodward (2001) states that the question of doubt about how consent should be applied to a patient's medical records can be resolved by policies that state what will and will not be covered. When a patient provides their PII to the primary health care provider on the basis of a set of preferences and a given policy, then they expect their PII to be treated as though they had entered a contract (Agrawal & Johnson, 2007). However, Grandison and Bhatti (2010) warn that often the wording of policies is purposely vague when detailing who the authorised users are who can access the patient records. This may be to allow unrestricted access to the records for ease of use, or to avoid litigation should a breach occur (Grams & Moyer, 1997). However, if a policy allows for the transfer of PII, then the patient would expect that the terms of the consent are followed by any future entities handling their PII (Agrawal & Johnson, 2007). Often government regulations may detail how consent is to be achieved, or the course of action to take when consent is not possible, such as the de-identification of patient records when shared for medical research (Appari & Johnson, 2010).

Whitley (2009) cautions that although patients are given the option of informed consent[21], many will not bother to read or understand the privacy notices, and merely accept what is presented to them. They do this in part because the task is perceived to be too complex, when in fact this may not be the case (Whitley, 2009). The result is that patients can then not fully comprehend and evaluate how their PII will be used in the future, and thereby lose control (Solove, 2008).

[21] Informed consent seeks to get answers to the following questions from the patient: What is to be included in the records? Who is the information going to be shared with?

When a patient finds that they have provided the incorrect type of consent, then they may want to revoke their consent. For example, a patient may decide to change their consent, such that they revoke the right to: use their data for medical research; hold personal data; and, use the personal data for a particular purpose (Whitley, 2009).

The next section will briefly consider the errors that can occur when medical records are processed in a primary health care facility.

4.5.2. Errors in Patient Information

Terry and Francis (2007) state, that when information in the patient record is incomplete or incorrect, it will adversely affect the treatment of that patient. Therefore, it is vital that the patient record is accurate, which means that it is free of mistakes and errors (Whitman & Mattord, 2009). If the content of the patient record is intentionally or unintentionally modified then it cannot be said to be accurate (Whitman & Mattord, 2009; Agrawal & Johnson, 2007; Terry & Francis, 2007).

Terry and Francis (2007) suggest that patients should check their EMRs where they can to ensure the accuracy of what is recorded. At a bare minimum, the patient should check to see that their 'patient choice model' detailing their preferred consent regime is active to avoid conflicts occurring.

When health care personnel are capturing and handling EMRs, they should ensure that the following six key attributes of good quality data are present[22], namely:

- ***Accuracy***, where patient data is accurately recorded by the health care personnel for the intended purpose, and only at the point where it is intended, so that it is not duplicated.

[22] The six key data quality attributes were chosen for their significance to the research project from an exhaustive list of those identified in Flowerday and von Solms, (2007). The six chosen do not represent the only data quality attributes that may apply to a given health care context.

- ***Validity***, where patient data is expected to be recorded in such a way that it complies with given regulations and/or the consent provided by the patient.
- ***Reliability***, where patient data is consistently collected, so that the process associated with its collection and dissemination is understood and followed by the health care personnel.
- ***Timeliness***, where patient data is captured directly after a treatment, so that it is available for immediate use should a further treatment be required.
- ***Relevance***, where patient data is only collected for an intended purpose and no unnecessary data is collected.
- ***Completeness***, where the health care personnel record all the relevant patient data as required for the treatment process and to meet compliance requirements from the state and professional bodies.

There are noticeable similarities in the qualities of patient data listed above and the various requirement for regulating data that were discussed at the end of Chapters Two and Three.

Terry and Francis (2007) suggest that the integrity of the patient data needs to be ensured by using various methods of authentication and having active audit trails and tracking mechanisms. Grandison and Bhatti (2010) state that audit trails are an important means to know if a patient record has been amended without the appropriate authorisation or due to a breach. However, they caution that often the audit feature is deactivated on the system, or was never put in use. This is problematic, because according to various legislative requirements patients should be informed if their records have been compromised (Appari & Johnson, 2010). Ironically, sometimes they are informed that it has been accessed, but not why or by whom the access occurred (Woodward, 2001).

McCallister, et al., (2010) caution that even though corrections to patient information may occur, it is important to know by whom, where, when and how that correction

was made. The next section will consider the concern around unauthorised access to patient information.

4.5.3. Unauthorised Access to Patient Information

Angst and Agarwal (2009) state that the chances of unauthorised access occurring to patient information is increased by the move from paper to electronic records. With paper-based records it was just a matter of securing a room and a physical log could be kept of who signed out a record, but with electronic records unauthorised access could be gained by a person on the other side of the globe (Agrawal & Johnson, 2007). It is likely that the patient can be unaware that their information has been breached and some form of identity theft has occurred (Terry & Francis, 2007). However, when a breach is discovered, the patient should be notified immediately, so they can take any necessary action to protect themselves from any privacy harms that may occur (McCallister, et al., 2010; Solove, 2008).

Lederman (2005) identified a number of problems that can possibly lead to unauthorised access to patient records when she was researching the adoption of digitised records in a hospital. These can be identified as follows:

- ***Non-integrated databases across the hospital***, which results in departmental silos that cannot be adequately secured and patient privacy cannot be guaranteed, as the location of all patient data is not known.
- ***Continued use of paper-based records instead of the existing EMR system***, which can lead to privacy violations, because paper-based records make it more difficult to comply with legislative privacy principles associated with compliance for access, completion, and correction.
- ***Poor security over system data*** means that specific controls such as timed log-offs and audit trails are not active on the system.

- ***Lack of restrictions on removing files from the primary health care facility***, through copying or uploading files to a remote site could lead to disclosure or loss when it leaves the premises.
- ***Access to irrelevant information*** should be managed though access restrictions where primary health care facilities share facilities with other medical entities.

Lederman (2005) reports that some primary health care facilities may have the required control mechanisms built into their systems and are just not using them. Other facilities have systems with none of the required functionality for information security control mechanisms, which perpetuates data losses (Lederman, 2005).

The Ponemon Institute annual study of patient privacy and data security conducted at 80 health care organisations in the US and comprising 324 interviews had the following key research findings (Ponemon Institute, 2012, p. 3):

- 94% of organisations in the study have experienced a data breach in the last two years. 46% report over five breaches in two years (*cf.* Figure 4.4).
- 2769 is the average number of records lost or stolen; with these typically being medical records, accounts (billing), and medical aid (insurance) details.
- The top three causes for a data breach are – lost/stolen computing devices, employee mistakes and third-party snafus (*cf.* Figure 4.5).

However, the unauthorised access to a patient's EMR can occur in a number of different ways and result in the potential loss of privacy and data. Figure 4.4 provides an overview of the kinds of loss and thefts of data that can occur. This is further detailed by identifying the incident that led to the data loss or theft as shown in Figure 4.5.

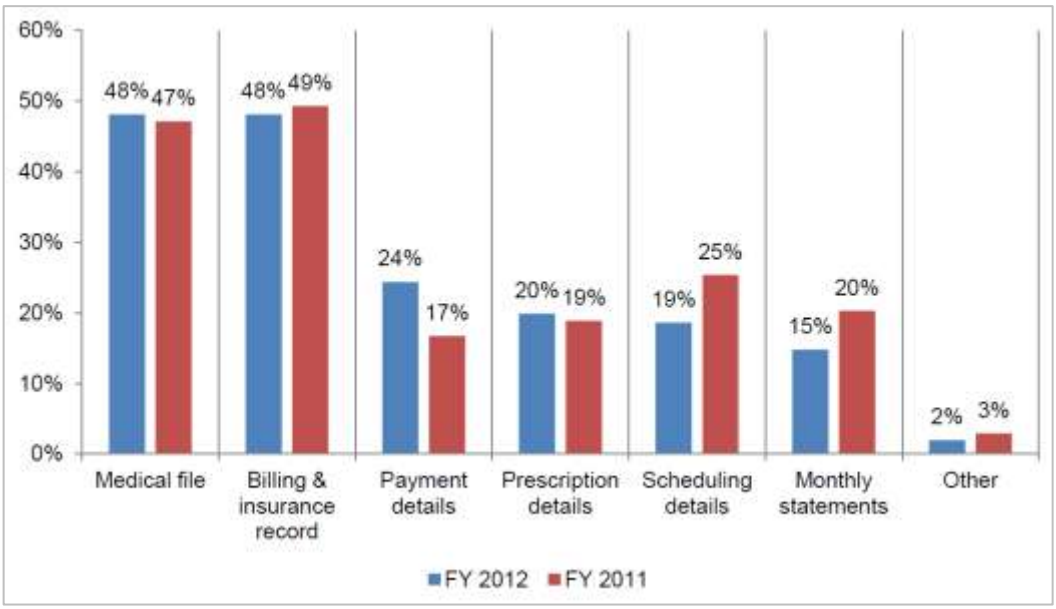


Figure 4.4: Reported data loss and theft - primary health care facilities (Ponemon Institute, 2012)

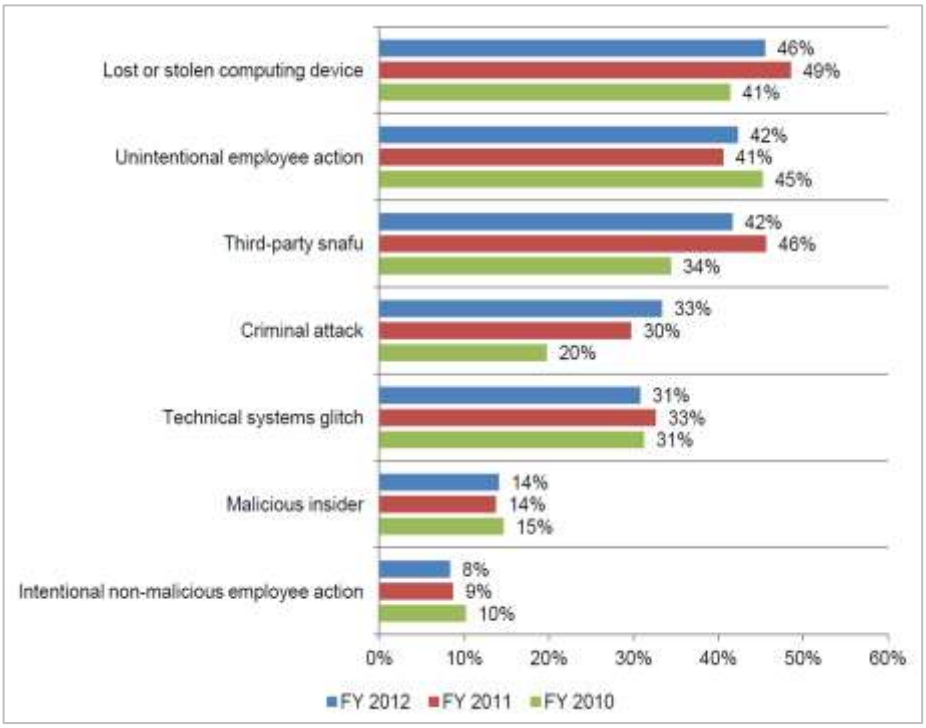


Figure 4.5: Nature of the incident - primary health care facilities (Ponemon Institute, 2012)

From the data represented in Figure 4.5, it is possible to deduce that health care personnel negligence appears to be the main culprit in the data loss. Third-party 'snafu' (error) also is also a significant contributor.

Petronio and Reierson (2009) support the establishment of access roles to restrict the flow of private information within the collective primary care boundaries thereby making it more likely that co-owners can control and regulate the flows to third parties. The boundary insiders would have more access, and be 'in the know', whereas boundary outsiders would be managed with the privacy rules associated with legislation.

However, this does not address how to avoid health care personnel negligence with respect to privacy and confidentiality. Lederman (2005) warns that what patients and health care personnel understand privacy to mean is often quite different from the legislative requirements.

Deshefy-Longhi, et al.'s (2004) suggestions on how to ensure that a patient's EMR are kept private and confidential are summarised as follows:

- Health care providers must seek to understand informational privacy, so that they can acknowledge their own and their patients' rights and concerns about privacy and confidentiality. This should be achieved by being aware of the current legislative requirements with regard to managing patient data. The knowledge gained should inform the development of protocols to protect informational privacy. These protocols should be communicated to patients in a manner that is understandable.
- Health care providers must determine their patients' level of understanding of informational privacy, and improve it if needed. This is especially important, so that it is possible to avoid patients making uninformed choices regarding consent at their initial contact point with the health care provider.
- Health care providers must ensure that their health care personnel are educated and informed about patient concerns and issues regarding privacy and confidentiality of health care information.

The final section in this chapter will briefly explore how the cultivation of a security culture could influence the ability to realise the three suggestions provided by Deshefy-Longhi, et al. (2004). The need to explore the notion of a security culture can be linked to the requirements of the PoPI Bill/Act (SA Justice Dept, 2009) and the ISO/IEC 29100:2011(E) standard, which detail how PPI compliance impacts on an individual's accountable for the misuse thereof. The patient also needs to be aware of the limitations that exist with protecting their PII, and the notion of informed consent implies that they have understood the relevant security issues. Therefore, it is assumed that unless a security culture is cultivated it is not possible to meet one of the key privacy principles, namely: accountability.

4.6. Cultivating a Security Culture

Whitman and Mattord (2009) believe that people are an important layer of security that can make a significant impact towards avoiding unauthorised access and use of private information. Conversely, if people are not made aware of the threat they can pose to security, they may be the cause of future security incidents[23] (Ciampa, 2010). Therefore, it is important that people should be cognisant of their impact on security within the organisation based on the roles they carry out on a day-to-day basis.

The OECD provides nine general security principles that are considered to cumulatively foster a security culture on a given computer network (OECD, 2002). These security principles are detailed in Table 4.1 and have general application to improving the security culture at a primary health care facility.

The various principles listed in Table 4.1 need to work together and not in isolation to ensure that a security culture is cultivated. Security forms the starting point of a learning continuum, which sees the recipient of the security information moving from *awareness*, to *understanding*, to *training*, and then *education* (Herold, 2011).

[23] (*cf.* Figure 4.5)

Awareness occurs in the presence of a passive recipient, where information is shared for informative purposes (Ciampa, 2010).

Table 4.1: Principles for the security of information systems and networks (OECD, 2002, pp. 10-12)

#	Principles	Description
1	Awareness	Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2	Responsibility	All participants are responsible for the security of information systems and networks.
3	Response	Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4	Ethics	Participants should respect the legitimate interests of others.
5	Democracy	The security of information systems and networks should be compatible with essential values of a democratic society.
6	Risk assessment	Participants should conduct risk assessments.
7	Security design and implementation	Participants should incorporate security as an essential element of information systems and networks.
8	Security management	Participants should adopt a comprehensive approach to security management.
9	Reassessment	Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The existing security policies, and/or a security topic of relevance are communicated to the staff in the organisation at this time. The second step requires *understanding*, which involves the recipient of the information becoming familiar with a given security topic. The third step, *training*, sees an individual becoming an active participant in the learning process. Finally, *education* refers to the ability of the recipient to internalise the information and actively interrogate it for greater insight. The learning continuum is not necessarily linear, but iterative, because new information may require retraining in a specific area. The McCumber INFOSEC Model highlights the importance of the training and education of staff as a crucial countermeasure against breaches in information security (Maconachy, Schou, Ragsdale, & Welch, 2001).

Finally, if health care personnel are informed about the various risks in the primary care setting with respect to the information privacy of the patient, they will be more effective as an added level of security. Furthermore, they will be able to better inform the patients of their choices with respect to accessing of their PII. Ultimately, the staff could be held accountable, because they would be informed of their fiduciary expectations with respect to keeping patient records confidential.

4.7 Conclusion

This chapter discussed the notion of accessibility by focusing on the four common concerns for information privacy, namely: collection, errors, unauthorised use, and secondary use. These were applied to the social perspective of the Socio-Technical Theory, after discussing the technical and environmental perspective within the context of health care. That discussion detailed the structure of the health care environment and the benefits of increasingly moving towards EMRs.

The discussion of the social aspects of the CFIP associated with collecting patient information, errors in patient information, and authorised access to patient information were expanded on and have direct relevance to the principles detailed in privacy legislation and the ISO/IEC 29100:2011(E) privacy standard. It is implied by the legislation, regulations and standards, that if the principles are understood the CFIP can be avoided. This is expected in part, to be accomplished by focusing on the notions of consent and control, and how they impact on accessibility. Finally, the chapter concluded with a brief discussion of how a security culture may be cultivated, so that a greater awareness of information privacy can be fostered. The importance is not only to ensure that social controls can be established, but also to address the principle of accountability that arises when considering privacy compliance. The principle of accountability is of great importance in understanding how health care workers work with the electronic medical records of the patients.

From a theoretical perspective, the CPM Theory was implied by considering the issues surrounding Principle 4, which seeks to coordinate mutual privacy boundaries by

establishing clear PII preferences through implied consent. By doing so, the patient makes it known what PII they are willing to disclose to others. Principle 5, which dealt with boundary turbulence, was addressed through the discussion of the CFIP and the accessibility to EMR.

Furthermore, the underlying concept behind the Restricted Access / Limited Control (RALC) Theory is considered, which is a hybrid of the Restricted Access and Control Theories, that were discussed in Chapters Two and Three, respectively. In the RALC Theory, the notion of restricted access is associated with the concept of privacy, and the management of privacy with a system of limited control. This theory therefore implies that an individual's perception of the concept of privacy and the management of privacy cannot be considered in isolation, but are mutually inclusive. It is therefore, necessary that social controls are utilised to increase the information security awareness of individuals to ensure that privacy compliance can be realised. From the perspective of electronic medical records and the health care workers, this would mean that they need to be made aware about the constructs of privacy, but at the same time, they need to understand how to use the facilities available to manage privacy.

The next chapter details the research methodology followed to collect the data required to be analysed in order to inform the development of the ***proposed information privacy model***. The details of the analysis process followed are detailed in Chapter Six together with the discussion of the findings from the data collected and the recommended model.

CHAPTER FIVE: RESEARCH METHODOLOGY

CHAPTER ONE:
INTRODUCTION

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

- 5.1. Introduction
- 5.2. Research Paradigm
  - 5.2.1. Positivism
  - 5.2.2. Interpretivism
- 5.3. Research Design
- 5.4. Strategy of Inquiry
- 5.5. Data Generation Method
  - 5.5.1. The Interview Guide
  - 5.5.2. Respondents
  - 5.5.3. The Expert Review Process
  - 5.5.4. Research Process
- 5.6. Research Evaluation
- 5.7. Conclusion

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

5.1. Introduction

Research evolves from a presented problem that needs solving or an area of interest that elicits further exploration (Gregor, 2006). The nature of Information Systems research is that it is conducted in multi-disciplinary and multi-cultural contexts (Niehaves, 2007). However, information systems research can be distinguished from other fields of research through its concern with how artefacts may be used in human-machine systems (Gregor, 2006). The artefact could be manifested as a construct, model, method, or instantiation (Hevner, March, Park, & Ram, 2004; March & Smith, 1995). Gregor (2006) further defines an artefact as something that is reliant on human interaction for its existence.

Lee (2001, cited in Gregor, 2006) states that information systems research is not merely the investigation of either the social (human) system or technological (machine) system, nor the two in parallel, but more importantly the phenomenon (artefact) that arises from their interaction. The focus would then be on the whole system and how the sum of the elements of the system relates to the investigated phenomenon. Gregor (2006) argues that Information Systems research lends itself more to investigating phenomena from an open systems approach rather than a closed systems approach, because of the effect of irrelevant influences. These irrelevant influences arise from the dynamic relationship that the system being studied has with the environment in which it interacts and with other systems outside of themselves (Gregor, 2006). This is especially true for the research of the information privacy phenomenon and its application to the health informatics domain (Whetton, 2005). The information privacy phenomenon is multi-disciplinary and derived from the interpretations of many individuals living in the world (Smith, et al., 2011).

To be able to interpret the 'living world' from the point of view of other individuals and themselves, a researcher needs to adopt a given research philosophy in order to gain insight into the nature of the research project being conducted (de Vos, Strydom, Fouché, & Delport, 2005). According to Oates (2006), the process of investigating the presented research problem is to a large extent guided by a researcher's view of the

world and how it can be investigated. However, a researcher still needs to argue for the acceptance of their interpretation by presenting evidence to support their claims (von Solms & van Niekerk, 2011), which can initially be framed by stating how the research project was conducted.

This chapter will briefly discuss the nature of research paradigms. Thereafter, the quantitative, qualitative and mixed methods to research design will be briefly described. Next, the strategy of inquiry that was utilised to conduct and manage this research project, namely the Design Science research guidelines are addressed. Finally, the data generation techniques utilised for this research project are explored, and the determinants of quality in research are highlighted.

5.2. Research Paradigm

A paradigm presents a set of beliefs held by the individual about the world and their relative role in it (Guba & Lincoln, 1994). This is not dissimilar to how an individual may consider the various elements in a given setting and reach an interpretation of say privacy, confidentiality, or trust. A paradigm is therefore understood as a unique worldview based on assumptions associated with the way we acquire knowledge about it (*epistemology*) and the very nature of our views of the world (*ontology*) (Oates, 2006; Niehaves, 2007). Creswell (2009) states that the discipline area, beliefs, and previous research conducted influence one's worldview. However, the very philosophical nature of a discussion of research paradigms raises divergent views of the research paradigms available, especially with choosing the 'right one' for the given discipline. De Vos et al. (2005) argue that it is not uncommon for a variety of competing paradigms to be found in any given discipline.

Guba and Lincoln (1994, p. 105) propose that four paradigms can be identified for "informing and guiding inquiry: positivism, post-positivism, critical theory and related theories, and constructivism". Constructivism or social constructivism is often associated with interpretivism (Creswell, 2009). The naming of paradigms may differ and their perceived importance may vary, but the three main paradigms that have

received the most focus over time have been positivism, interpretivism, and critical theory (de Vos, et al., 2005). Oates (2006, p. 283) argues that each paradigm could be further divided and that "each of these have different assumptions about the nature of reality, the purpose of research and what counts as knowledge".

Figure 5.1 depicts a continuum to represent the variances of reality between positivism and interpretivism within the social sciences. This expanded view of the continuum clearly shows 'reality as social construction', as having its own position on the continuum, and not simply the same thing as interpretivism. Research conducted in information systems often makes use of the social sciences to assist in the placement of research into what appears to be an irregular and uncertain world in which we live (Gregor, 2006).

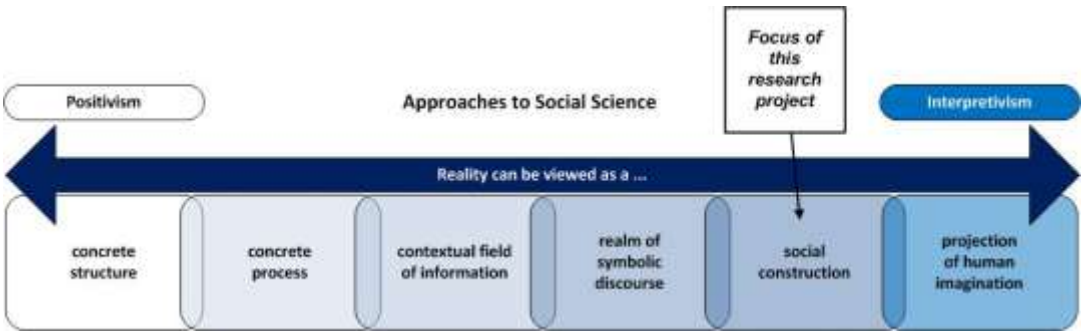


Figure 5.1: Positivism-Interpretivism continuum (adapted from Morgan & Smircich, 1980)

Niehaves and Stahl (2006) argue that there are various other paradigm permutations available, and that assuming a research paradigm is merely a coin toss with either a positivistic or interpretivist outcome limits the possibility for exploring other options. Subsequently, Niehaves and Stahl (2006) state that the term paradigm is not always used to refer to a particular epistemological stance, but also seeks to address distinct phases of a problem-orientated process, such that it can be understood and solved. Niehaves and Stahl's (2006) discussion originates from the introduction of two distinct paradigms into the milieu, namely behavioural science research (*a problem understanding paradigm*) and Design Science research (*a problem solving paradigm*). However, Niehaves (2007, p. 8) argues "against the seemingly common perception that Design Science would be a 'third paradigm' amounting to positivism and

interpretivism", but rather "that issues of epistemology and Design Science research (evaluation) are intrinsically intertwined". The relationship between Behavioural Science research and Design Science research can be viewed as circular by nature and similar to the notion of the hermeneutic circle. This refers to understanding leading to interpretation, which in turn leads to further understanding. We see in Figure 5.2 that Behavioural Science research is concerned with interpreting an artefact that has been developed with Design Science research (Hevner, 2012). Therefore, behavioural science research focuses on determining if an artefact provided value. The outcome then of the behavioural science research is that it provides theoretical insights to Design Science research that assists in improving existing or developing new artefacts. Similarly, the investigation of the constructs of this research project, namely: privacy, confidentiality and trust – lead to an improved understanding of why individuals may behave as they do. With this knowledge in hand, it becomes easier to develop an artefact, i.e. the information privacy model in order to raise information security awareness, which in turn is expected to influence the behaviour of those exposed to the model.

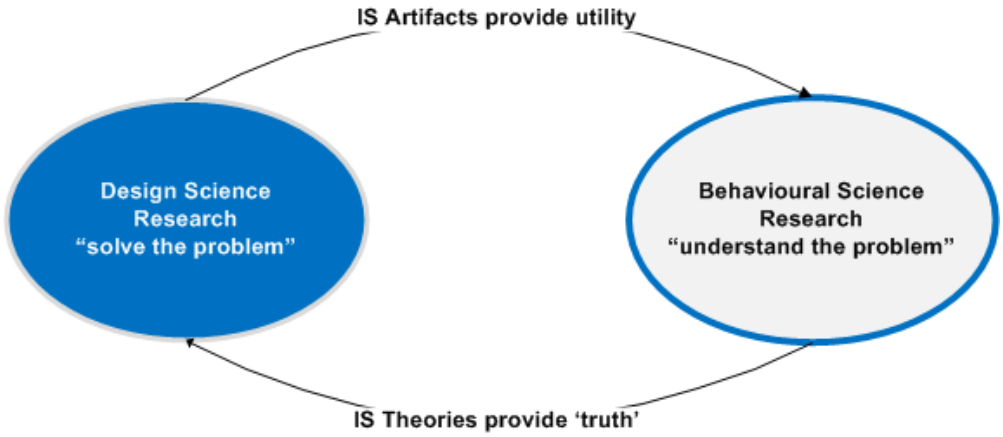


Figure 5.2: Circular relationship of Design Science and Behavioural Science Research (Hevner, 2012)

It is apparent that multiple philosophical stances are possible and that any one or a combination of these can be adopted when conducting Information Systems research. Furthermore, it can be seen that some, e.g. Design Science research can not only be considered as a paradigm, but also as the strategy of inquiry to be used for evaluating an artefact. The focus of the discussion to follow will be on the traditional paradigms

of positivism and interpretivism in order to provide a background for the choice of the chosen paradigm for this research project.

5.2.1. Positivism

Positivism is synonymous with the natural scientific method where the world is viewed in a systematic manner that does not recognise randomness (Oates, 2006). The ontological assumption is that reality is meaningless, which refers to it being independent of human basic emotions. Any social phenomenon that is investigated is then treated as though it was a physical object. Therefore, the social world exists externally and is viewed objectively (Blumberg, Cooper, & Schindler, 2008). Healy and Perry (2000, cited in Krauss, 2005) use the analogy of a 'one way mirror' to explain a researcher's view of the world. The epistemological assumption is then that it is possible to measure the knowledge acquired whilst observing the research phenomenon, because any data analysis is free of influence, i.e. a researcher is behind the "one way mirror". Trochim (2000, cited in Krauss, 2005) clarifies that nothing that is happening outside of the observed behaviour is relevant for a positivist researcher for the study they are conducting. Klein and Myers (1999, p. 69) summarise a positivist approach to information systems research by stating that it exists, "if there is evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about the phenomenon from a representative sample to a stated population".

Oates (2006) states that positivism is associated with three basic techniques, namely:

- ***Reductionism***, which seeks to reduce complex systems to their smallest measurable unit, so that it is easier to study the sum of the units in relation to a given complex system.
- ***Repeatability***, which focuses on repeating the research to determine that the study was conducted in an objective manner that was free of researcher bias.

- ***Refutation***, which is concerned whether or not other researchers who have repeated the research were able to obtain the same results. If not, then they would refute the original results.

Krauss (2005) sees positivism as a means of understanding the true nature of the world, so that it can be predicted and controlled. The prediction and control is realised through the generalisation of findings once they have been found to be true or not. However, Oates (2006) argues that it becomes increasingly difficult to predict and control settings when researching people, because their interactions in the world in some way influence a given phenomenon. Arguably, positivist researchers often focus only on one explanation to describe or understand a phenomenon (Blumberg, et al., 2008), but this can also result in the researcher missing other explanations originating in the environment (Oates, 2006).

The positivist philosophical stance is perhaps not suitable when the phenomenon being researched is embedded in the social world of thinking and feeling people (Whetton, 2005). An initial criticism of positivism is that reducing the phenomenon to too small an element may result in the larger context being overlooked. Within the context of this research project, it becomes increasingly difficult to improve awareness of the elements of information privacy without creating a holistic view of privacy and how the various elements identified in Chapter Two interact. From a health care worker's perspective, breaking the elements of information privacy down into its individual elements would aid awareness and understanding, but they would still need to see the impact on the overall system.

A further criticism of positivism is associated with the need for replication in research. It is argued that it is also increasingly difficult in the social world for all the converging characteristics to be identical without manipulating the setting. Subsequently the quest for generalisation often ignores the unique qualities or the context of a social phenomenon (Oates, 2006).

It seems apparent, that specifically in those disciplines with a dominant social sciences element, that a researcher should increasingly look at the settings and people holistically, so that the people, settings, or groups are not reduced to mere variables, but are viewed as a whole. This provides a greater opportunity to describe the actions of individual elements interacting with the system (Gregor, 2006).

There is an increasing paradigm shift from positivism to interpretivism as valid approaches for information systems research (Avgerou, 2000). Interpretivism has the potential to provide deeper insights into an information systems phenomenon (Klein & Myers, 1999). The origin of the deeper insight is an interpretivist researcher's ability to apply critical thought while viewing the world subjectively. In order to better understand interpretivism, it will be discussed in the section to follow.

5.2.2. Interpretivism

Klein and Myers (1999) raise concern that the word "qualitative" is often seen to be synonymous with interpretivism, but this should not be the case, as a qualitative conceptual framework could be used in any existing paradigm. Oates (2006, p.292) states that "interpretive research in information systems and computing is concerned with understanding the social context of an information system". The interpretivist view of the world is that individuals give meaning to the world by being part of the social world and removing oneself from the social world removes part of that meaning (Creswell, 2009; Blumberg, et al., 2008).

Therefore, the characteristics of the individual living in the world cannot simply be reduced to a set of independent objects as put forward by positivists. Rather the phenomena need to be understood as being dependent on human interests (Creswell, 2009). Habermas (1970, cited in Blumberg et al., 2008, p. 21) proposed that "human interests not only channel our thinking, but also guide how we investigate the world *(i.e. which questions we ask)*, and how we construct our knowledge *(i.e. how we formulate the answers found)*". Therefore, the context in which phenomena are being studied adds value (Klein & Myers, 1999).

Packer and Addison (1989, p. 19) state that "interpretive inquiry focuses on human activity situated in context and the offspring of such activity: institutions, histories, accounts, records, texts, stories, lives". The goal of the inquiry aims to understand the cultural and historical viewpoints of individual participants (Creswell, 2009). Klein and Myers (1999) divide the process of knowledge acquisition of a phenomenon into preconceptions of a researcher and participants, and the common interpretations that evolve from their interaction. Table 5.1 identifies and describes the seven principles.

Table 5.1: Principles for Interpretive Research fieldwork (Klein & Myers, 1999, p. 72)

Interpretive Research Principles
1. Principle of the Hermeneutic Circle
This principle suggests that all human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form. This principle of human understanding is fundamental to all other principles.
2. Principle of Contextualisation
Requires critical reflection of the social and historical background of the research setting, so that the intended audience can see how the current situation under investigation emerged.
3. Principle of Interaction Between the Researchers and the Subjects
Requires critical reflection of how the research materials (or 'data) were socially constructed through the interaction between the researcher and the participants.
4. Principle of Abstraction and Generalisation
Requires relating the idiographic details revealed by the data interpretation through the application of principles 1 and 2 to theoretical, general concepts that describe the nature of human understanding and social action.
5. Principle of Dialogical Reasoning
Requires sensitivity to possible contradictions between theoretical preconceptions guiding the research design and actual findings ('the story which the data tell') with subsequent cycles of revision.
6. Principle of Multiple Interpretations
Requires sensitivity to possible differences in interpretations among the participants as are typically expressed in multiple narratives or stories of the same sequence of events under study. Similar to multiple witness accounts even if all tell it as they saw it.
7. Principle of Suspicion
Requires sensitivity to possible 'biases' and systematic 'distortions' in the narratives collected from participants.

They argue that interpretive research using case studies and ethnographic studies must be conducted and evaluated against a set of *Principles of Interpretive Research*, but these principles can also apply to other strategies of inquiry (Klein & Myers, 1999).

Oates (2006, p. 292) identified a number of characteristics which she believed are indicative of the interpretivist paradigm, and where applicable these have been associated with the principles listed in Table 5.1. These characteristics include:

- ***Multiple subjective realities*:** the individual perceptions of individuals or groups do not presuppose a positivistic universal truth, but rather 'truth' is constructed from their cultural viewpoint of the world in which they live. **[Principle 1 & 6]**
- ***Dynamic, socially constructed meaning:*** the perceptions of reality realised by an individual or a group remain dynamic if they are shared with others by using some form of communication medium that conveys their meaning and understanding. **[Principle 1 & 4]**
- ***Research reflexivity*:** the researcher needs to be cognisant of the fact that they bring innate bias to a research project and therefore need to reflect on their assumptions, beliefs, values and actions during the process of the research. **[Principle 1, 3 & 7]**
- ***Study of people in their natural social setting*:** the researcher does not view people in an artificial setting through a "one way mirror", but seeks to understand how they are immersed in their natural environment in order to ensure a holistic viewpoint to the research. **[Principle 1 & 2]**
- ***Qualitative data analysis*:** the collection and analysis of the use of language, metaphors, and visual representations is often done with the aid of qualitative data. **[Principle 1 & 5]**
- ***Multiple interpretations*:** unlike the positivist researcher, there are multiple explanations that arise from the research conducted. Whether a single explanation has a greater utility over any others will depend how much evidence there is in support of it. **[Principle 1 & 6]**

We have established that interpretive research can be a valuable way to identify the attitudes and beliefs of individuals and groups about a phenomenon in a given context. Whetton (2005) states that gaining insights into how people interpret and respond to health informatics programs and initiatives assists in learning what is relevant and meaningful from their perspectives. From a health informatics perspective it can result in a richer understanding of information management concerns associated with privacy, confidentiality, and issues surrounding the sharing and accessing of health records (Appari & Johnson, 2010). Patients, health care practitioners, and health care workers would be able to reach common understanding of how information privacy applies to their daily work processes by reviewing the model presented in this research project. How they interpret the model will assist in increasing their awareness of information security within a given primary health care facility.

This research project focused on the interpretive paradigm and more specifically the variant of social construction. A social constructionist works on the assumption that individuals want to understand the world in which they live and work (Creswell, 2009). These assumptions rely on the individual participants to provide as much rich information as possible. Appari and Johnson (2010) suggest that qualitative methods can be utilised most effectively in collecting health informatics information. However, Coiera (2003, cited in Whetton, 2005) argues that the predominance of qualitative research over quantitative research weakens research in the health informatics discipline. Martella, Nelson and Machand-Martella (1998) state that researchers often attempt to discount research methods in a research design other than their own, rather than identify their merits. There is thus an ongoing debate as to which research design is the most appropriate. The next section will briefly describe the research design options available.

5.3. Research Design

We have identified *social construction* as the 'interpretive' paradigm of choice for this research project, because it supports collecting multiple viewpoints on the research

phenomenon, i.e. the information privacy of a patient. Determining the paradigm is a starting point, but how the research is to be designed requires a conceptual framework for a researcher to make explicit how the research topic was investigated and the process followed (Oates, 2006). There are three possible research designs that can be utilised, namely: quantitative, qualitative, and mixed research design. De Vos et al. (2005, p. 75) provide a tabular comparison of the quantitative and qualitative approaches to research design in social research (Table 5.2).

Table 5.2: Quantitative and Qualitative Approaches in Social Research (de Vos, et al., 2005)

Quantitative approach	Qualitative approach
Epistemological roots in positivism	Epistemological roots in interpretivism
Purpose is testing predictive and cause-effect hypothesis about social reality	Purpose is constructing detailed descriptions of social reality
Methods utilise deductive logic	Methods utilise inductive logic
Suitable for a study of phenomena which are conceptually and theoretically well developed; seeks to control the phenomenon	Participants' natural language is used in order to come to a genuine understanding of their world
Research design is standardised, fixed and replicable	Research design is flexible, unique and evolves throughout the research process. No fixed steps and design completely replicable
Data are obtained systematically and in a standardised manner	Data sources are determined by information richness of settings
The unit of analysis is variables which are atomistic (elements that form part of the whole)	The unit of analysis is holistic, concentrating on the relationships between elements, contexts, etc. The whole is always more than the sum

Johnson and Onwuegbuzie (2004, p. 15) argue that "differences in epistemological beliefs should not prevent a qualitative researcher from utilising data collection methods more typically associated with quantitative research and vice versa". Green, Caracelli, and Graham (1989, cited in Creswell, 2009) state that the utilisation of multiple methods has the benefit of one method informing another. A mixed research design would therefore contain elements of the quantitative and qualitative research design.

The three research designs (quantitative, qualitative and mixed) have been briefly explained, so that the reasoning for choosing a qualitative research design was made more explicit. The depiction of the research arc in Figure 5.3 provides a means to

graphically represent the conceptual framework of this research project. For clarity, it should be restated that the goal of this research project is to provide a model of information privacy that could be utilised in the health informatics domain as a starting point to assist in improving stakeholder awareness of information privacy issues.

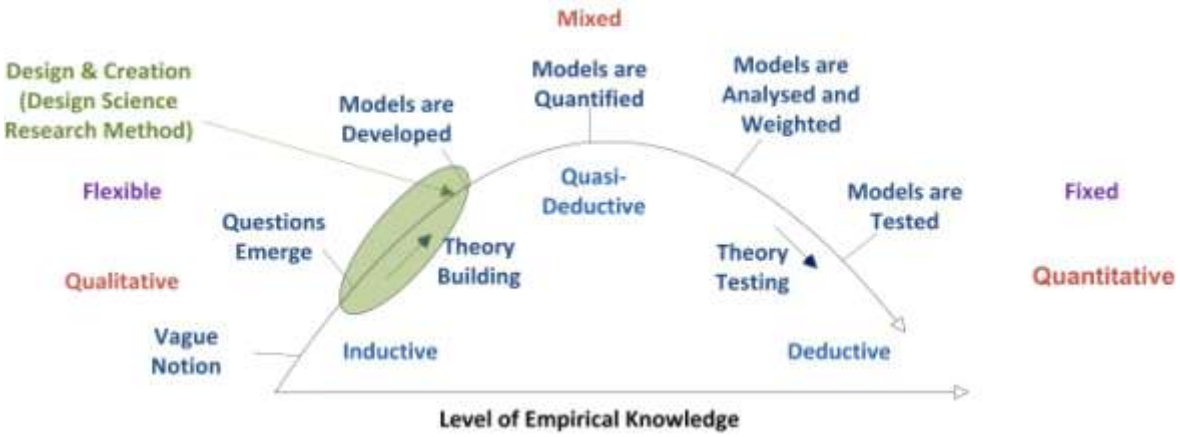


Figure 5.3: Informational privacy model applied to a research arc (adapted from Latham, 2005)

This research project is conceptually framed as falling within the research area shaded on the research arc (*cf.* Figure 5.3). The research project thus makes use of a qualitative research design, which allows for flexibility of the way in which the research is conducted. The flexibility requires inductive logic to be applied to aid in providing a plausible solution to the research question under review. The strategy of inquiry or methodology used in the shaded area is referred to as *design and creation* (Oates, 2006) or the Design Science research method (Hevner, et al., 2004).

The discussion earlier in this chapter identified that Design Science is viewed by some as a paradigm (Niehaves, 2007). Oates (2006) addresses the Design Science problem-solving nature of artefact design and creation, but does not relegate it to the level of a paradigm, but rather a research strategy. This research project adopts the stance that Design Science research can be applied as a strategy of inquiry within the interpretive paradigm. Von Solms and van Niekerk (2011) argue that choices of methodology need not be restricted to traditional approaches. The next section will discuss the use of Design Science research as the strategy of inquiry for this research.

5.4. Strategy of Inquiry

Creswell (2009) states that strategies of inquiry provide specific direction for procedures in a research design. The reason for stating the strategy of inquiry would assist future researchers in feeling confident that the findings of the research are credible (von Solms & van Niekerk, 2011). Therefore, the strategy of inquiry provides the approach to answer the research question (Oates, 2006). The strategy of inquiry for this research project will be guided by the research design chosen, i.e. qualitative research design.

Oates (2006) identifies five strategies for conducting qualitative research, namely: ethnography, action research, case study, survey, experiment, and design and creation. Of all of these approaches, design and creation is the most relevant for this research project as it is concerned with the development of a new IT product or artefact (Oates, 2006).

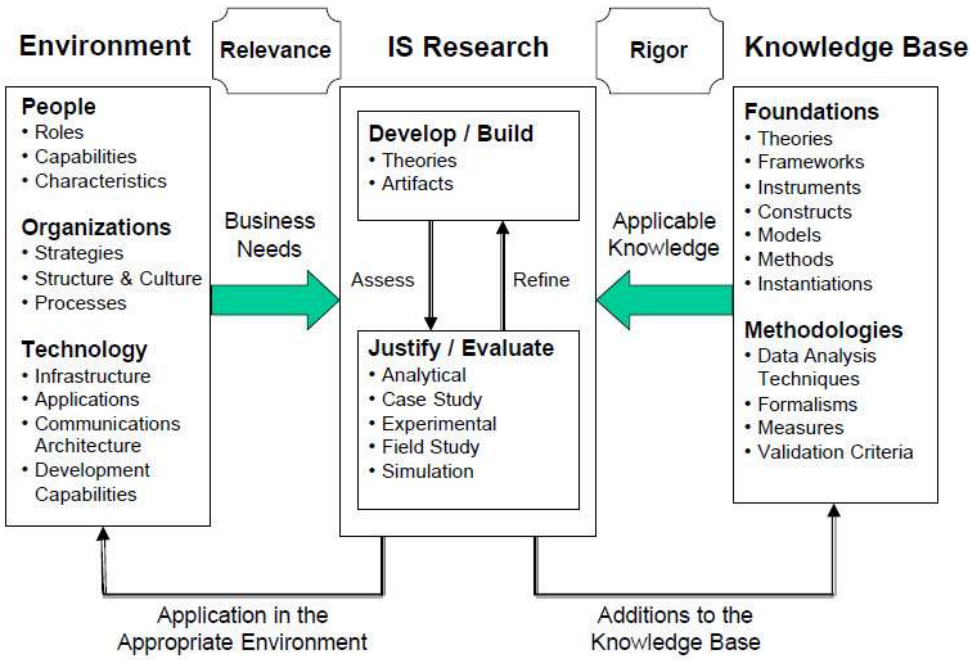


Figure 5.4: Information Systems Research Framework (Hevner, et al., 2004)

Hevner, et al. (2004) proposed an information systems research framework that can be used to frame Design Science research (*cf.* Figure 5.4). Typically, a researcher decides

on the context of the research and reviews the socio-technical elements of the environment. Within the context of this research, the broad environment is the health care sector and more specifically health informatics within primary care facilities. These facilities employ health care practitioners who make use of a manual or technical information system to share information for the treatment of patients. The sharing of information is crucial in this setting, but it also raises a specific business need that has to be met, i.e. information privacy. This need is then researched within the information systems discipline to derive a suitable artefact to be of relevance to the business need raised in the environment.

March and Smith (1995, p. 253) identified four types of artefacts as being produced during the design and creation strategy of inquiry. These artefacts are:

- ***constructs***, which provide the domain-specific language needed to define and communicate an identified problem and possible solution.
- ***models*** that combine the constructs in a manner that represents a real world situation and provide an understanding of the problem in order to develop a solution.
- ***methods*** or methodologies provide guidance on models that are to be developed and the stages to be followed when using IT to solve problems.
- ***instantiations*** are a demonstration of a working system which can be realised when a construct, model or method are actually implemented.

Furthermore, March and Smith (1995) state that build and design are the two basic activities found in Design Science. The artefact to be built for this research project is a model and it will be evaluated through iterative refinement by expert reviewers. These activities expound the notion that design is also about the process. The process of building the artefact does not necessarily follow a predefined set of steps. Similarly, the evaluation of the artefact is not prescriptive. This inherent flexibility to change artefacts and processes assists in managing complex problems.

The knowledge base of the research framework provides the theoretical catalyst indicative of the circular relationship between Design Science research and behavioural science research (*cf.* Figure 5.2). Privacy is not a new phenomenon, but has been promoting debate for decades (Schoeman, 2007). Therefore, there exists an extensive knowledge base that provides valuable direction and insights into the creation of the artefact for this research. Extracting information from the knowledge base provides rigor for building and evaluating the artefact. The outcome of this process is that the knowledge base both informs and is then informed in turn by the findings of the artefact design. Similarly, the artefact would be tested in the environment.

Oates (2006, p. 116) stated that "many computing researchers do not evaluate whether the artefact does work in the real-life context". A researcher's objective is to demonstrate a *'proof of concept'* via a functioning prototype that under certain conditions would act in a given manner. The focus is then not on the 'proof' typical of positivism, but rather an interpretivist researcher aims for plausibility (Oates, 2006). The goal of a researcher is then to act in a similar manner to a lawyer in a court case and ensure that the 'plausibility' of the data is based on evidence and not tainted or perceived to be tainted (von Solms & van Niekerk, 2011).

Ahmad, Guy & Wasana (2011) completed an exhaustive review of Design Science literature that identified multiple steps proposed by authors that needed to be completed to improve the 'plausibility' of the research process. Oates (2006) suggests adopting the five step iterative process proposed by Vaishnavi and Kuechler (2004), namely: awareness of a problem, suggestions on how to solve the problem, development of the artefact, evaluation of the worth of the artefact, and the conclusions derived from the results and shortcomings of the design processes are recorded.

However, Hevner, et al. (2004) similar to Klein and Myers (1999) principles for interpretive research provide seven guidelines/principles for 'best practice' Design Science research that should be followed. These guidelines are represented in Table

5.3., and brief descriptions *(shown in italics)* have been provided about how the guidelines apply to this research project. The guidelines should not be seen as strictly sequential, nor do they have to be present in all research projects (Hevner, et al., 2004).

Table 5.3: Guidelines for Design Science Research (adapted from Hevner, et al., 2004)

Guideline	Description
Guideline 1: Design as an Artefact	A viable artefact in the form of a construct, a model, a method, or an instantiation. ***The artefact for this research project is a model.***
Guideline 2: Problem/Relevance	To develop technology-based solutions to important and relevant business problems. ***The focus is on providing a holistic view of information privacy as it applies to health informatics, and specifically primary health care facilities.***
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well executed evaluation methods. ***An expert review process is used as a means of evaluating and informing the artefact design.***
Guideline 4: Research Contribution	To be effective it must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies. ***The model will extend the knowledge base relating to graphically representing compliance in information privacy.***
Guideline 5: Research Rigor	It relies on the application of rigorous methods in both the construction and evaluation of the design artefact. ***The artefact was created with extensive use of the existing research and evaluated through an expert review process.***
Guideline 6: Design as a Search Process	Use the resources available when developing an effective artefact while satisfying the laws of the problem environment. ***The principles and themes arising from an extensive review of privacy and health informatics have been used for this research project to develop the artefact.***
Guideline 7: Communication of Research	Present the research to audiences that are either technological-orientated or management-orientated. ***A part of this research has been communicated as a research -in-progress paper at a national conference, and is intended to be published in a journal.***

The information systems research framework and the guidelines for Design Science research proposed by Hevner, et al. (2004) provided the necessary finalisation to the discussion on the strategy of inquiry to be utilised for this research. In summary, the research project has utilised an interpretive paradigm with a qualitative conceptual framework and a Design Science research methodology. It is now necessary to

determine how the data generation will be accomplished in order to realise the final artefact.

5.5. Data Generation Method

Oates (2006) states that field data or evidence are produced by making use of a data generation method. This research project is being conducted from a qualitative conceptual framework, so the data collection tools that could be used include: interviews, observations, document review, visual data analysis, or questionnaires (Silverman, 2011). An interview data collection tool was used to get responses from individual experts and then a group interview was conducted with three of the respondents.

The interview is a commonly used means of collecting data in qualitative research (Silverman, 2011; de Vos, et al., 2005), and was chosen as a tool that could be used for refining and evaluating the artefact. This choice was influenced by the fact that the participants (experts) in the research had to provide constructive criticism of the artefact (model) as it might be applicable to real world settings.

5.5.1. The Interview Guide

The nature of this research project is that the constructs *(privacy, confidentiality and trust)* investigated are largely governed by individual perceptions. Blumberg, et al. (2008) suggest using semi-structured one-on-one interviews as a means to access individuals' *perceptions* on a given topic. The semi-structured interview is guided by an *interview guide approach*, which serves the purpose "as an appropriate instrument to engage the participant and design the narrative terrain" (Holstein & Gubrium, 1995, cited in de Vos et al. 2008, p. 296). The interview guide provides a means to ensure that all the themes (topics) to be covered are addressed. A researcher does not predefine a rigid set of questions to be answered, but rather the topics and open-ended questions serve as a means to frame the interview (Martella, et al., 1998).

Further questions can be used by the researcher to stimulate the responses (Skulmoski, Hartman, & Krahn, 2007).

The process followed to develop the interview guide is shown in Figure 5.5. The privacy requirements summary (*cf.* Table 2.2), ISO/IEC 29100 principles (*cf.* Table 2.5), Caldicott principles for confidentiality in primary care facilities (*cf.* Table 3.2), and the summary of the HPCSA guidelines (*cf.* Table 3.3) were utilised as a means to determine the general interview topics and questions to be covered during the interview process. A series of open-ended questions were then grouped into each topic to form the interview guide (Figure 5.6). During the refinement of the topics and interview questions, it became evident that the ISO/IEC 29100:2011(E) principles would be an effective way to sort the future analysis of the primary data. Subsequently, it was determined that the 11 principles contained in the ISO/IEC 29100:2011(E) would be used as the codes for the analysis, and mapped against the responses of the respondents. The application thereof can be seen in Chapter Six.

The interview guide was tested in a pilot session containing two respondents experienced in research design to determine if the question set and layout was appropriate for semi-structured interviews. The comments received from the pilot session respondents required a rework of the questions. Once the questions were reworked, they were again tested and refined with the assistance of the pilot respondents. Thereafter, the interview guide was administered as a tool for primary data collection for this research project. Martella, et al. (1998) stated that the interview guide (*cf.* Figure 5.6) provides a valuable tool when there is a need to collect similar information from the respondents.

The next section briefly considers the respondents that were involved in the research project and how their interaction assisted as a means of triangulating the primary data collected. The respondents also assisted in refining the artefact (information privacy model).

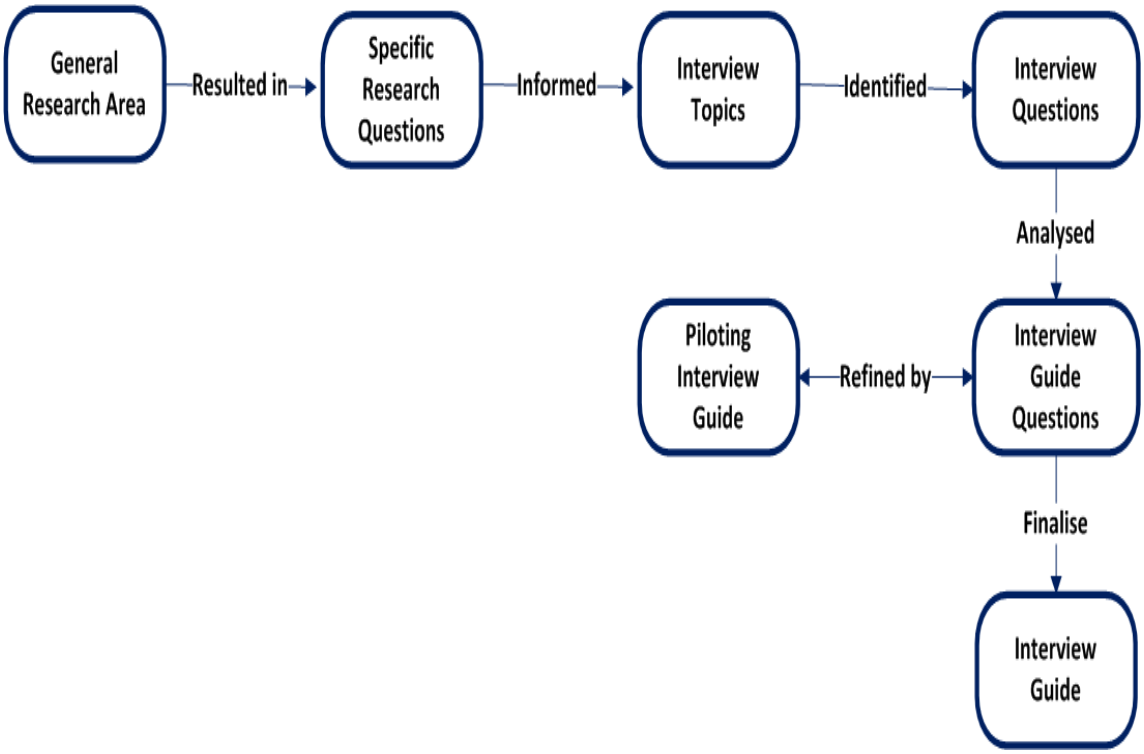
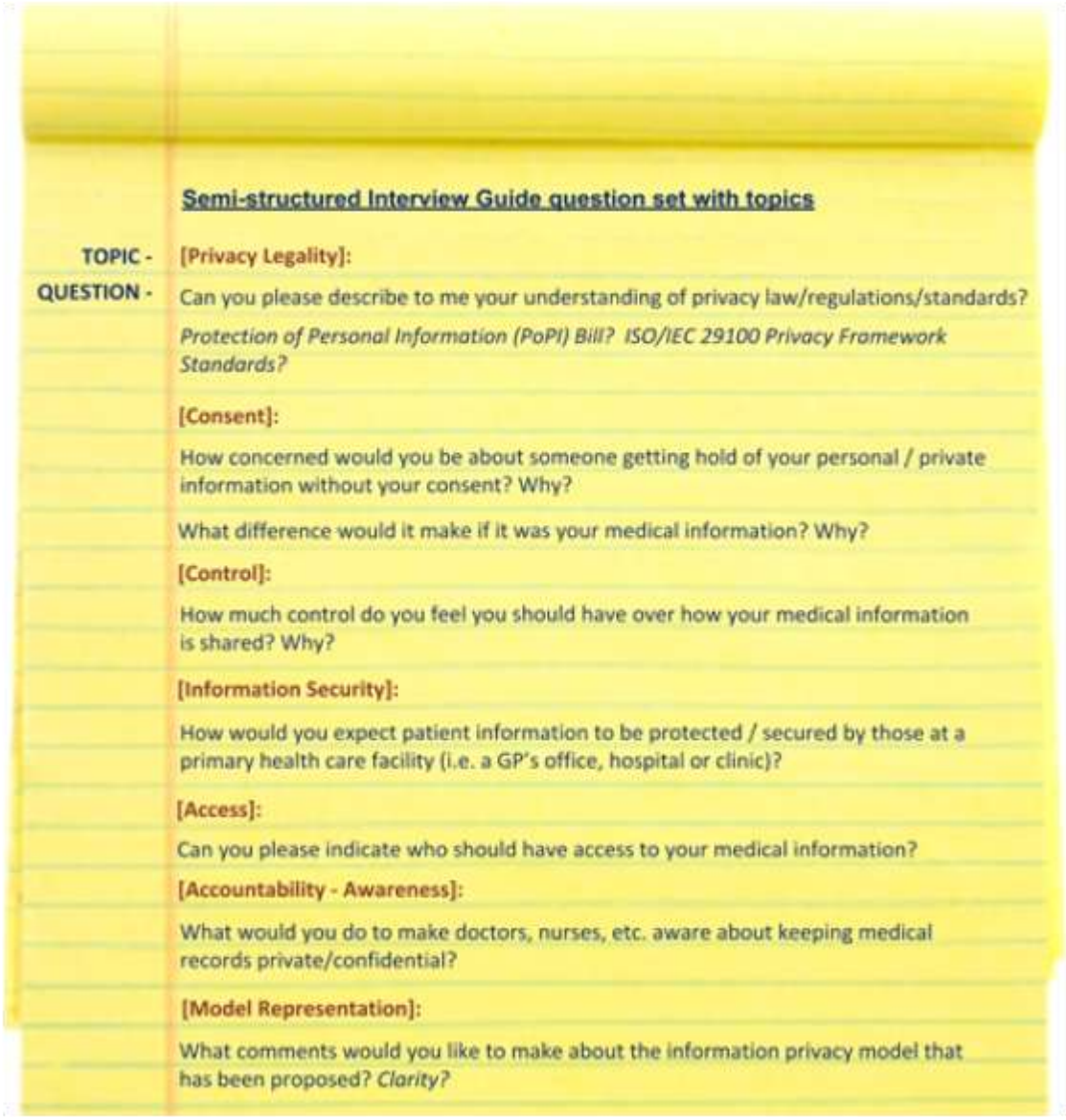


Figure 5.5: Development Process for the Interview Guide

5.5.2. Respondents

This research project made use of individual experts (respondents) in order to review the artefact and thus inform its further development. Experts provide different perspectives on a given problem area that may not have been evident without their participation (Skulmoski, et al., 2007). The experts were identified based on their skills and knowledge in the areas of health care, privacy, and information security. Their selection was guided by referrals from individuals who had engaged with them in a professional capacity. Three of the respondents were approached at a national information security conference, and they comprised the experts for Phase 1. The remaining experts were selected based on referrals received, and formed part of Phase 2 and 3. All of the experts interviewed were briefed on the expected outcome of the project, i.e. the development of an information privacy model, and their expected contribution to the process. The composition of the experts and the phases in which they participated in the research process are depicted in Table 5.4.



Semi-structured Interview Guide question set with topics

TOPIC - [Privacy Legality]:

QUESTION - Can you please describe to me your understanding of privacy law/regulations/standards?

Protection of Personal Information (PoPI) Bill? ISO/IEC 29100 Privacy Framework Standards?

[Consent]:

How concerned would you be about someone getting hold of your personal / private information without your consent? Why?

What difference would it make if it was your medical information? Why?

[Control]:

How much control do you feel you should have over how your medical information is shared? Why?

[Information Security]:

How would you expect patient information to be protected / secured by those at a primary health care facility (i.e. a GP's office, hospital or clinic)?

[Access]:

Can you please indicate who should have access to your medical information?

[Accountability - Awareness]:

What would you do to make doctors, nurses, etc. aware about keeping medical records private/confidential?

[Model Representation]:

What comments would you like to make about the information privacy model that has been proposed? *Clarity?*

Figure 5.6: Interview Guide Questions

Table 5.4: Composition of participating experts in the expert review process

Research Process		Area of Expertise		
Expert	Phase	Health care	Privacy	Information Security
EX1	1		☑	☑
EX2	1		☑	☑
EX3	1		☑	☑
EX4	2			☑
EX5	2 & 3	☑		☑
EX6	2 & 3	☑	☑	☑
EX7	2 & 3	☑		☑

The experts who participated in Phase 1 requested anonymity in the study, and consent was sought prior to administering the interview questions. A further consent was sought for the respondents for Phase 2 and 3. Phase 2 was conducted as individual interviews, and Phase 3 was conducted as a focus group. Morgan (1996) suggests mixing individual interviews with a focus group in order to clarify individual responses rather than simply aggregating the responses from individual interviews.

This research project made use of seven expert reviewers. Skulmoski, et al. (2007) suggests that the number of experts is really dependent on the purpose/aim of the research, or expected outcome.

5.5.3. The Expert Review Process

The expert review process followed was based on the principles of the Delphi technique. Skulmoski, et al., (2007) state that in principle the Delphi technique can take on many forms, but that as a minimum the researcher should meet certain design criteria when using this technique, or the results become questionable. Table 5.5 lists an application of the Delphi technique design criteria, as they applied to the expert review process conducted for this research.

5.5.4. Research Process

The application of the research process shown in Figure 5.7 will be briefly described within the context of primary and secondary data. Primary data in the context of this research project refers to the data collected from the three phases of the expert review process through administering the interview guide. Secondary data on the other hand refers to data that was previously recorded in studies that had been conducted. The results of those studies were used in order to determine the various elements that would be needed to be included in the artefact (information privacy model) that was being proposed within the health care context.

Table 5.5: Delphi technique design criteria principles (adapted from Skulmoski, et al., 2007)

Design Criteria	Description	Applied in this study
Methodological Choices	Typically quantitative, but also applied to qualitative and mixed research methods.	Interpretive -> Qualitative
Initial Question – Broad or Narrow	The questioning style can range on a continuum from open-ended (broad) to closed (narrow).	Initial semi-structured one-on-one questioning using specific topics for structuring and funnelling the process.
Expertise criteria	Participants need to: a) be knowledgeable and experienced on the issues under investigation, b) capacity and willingness to participate, c) sufficient time to participate, and d) effective communicators.	Each participant is considered an expert in one or more of the following areas: health care, information security, and/or privacy. They were all able to participate as required.
Number of participants	The researcher needs to decide between groups that are small and homogeneous or large and heterogeneous in size and design.	This study made use of a small homogeneous group of 7 respondents. 3 of the respondents were involved in 2 successive phases.
Number of rounds *(the term 'phases' was used for this research)*	The number of rounds is typically between 2 – 3 iterations, but more for heterogeneous groups, and less for homogeneous groups using qualitative methods. The number of phases is dependent on when sufficient information is acquired.	Three phases (P) were conducted for the purpose of this research. P1 = 3 participants P2 = 4 participants P3 = 3 participants *(returning)*
Mode of Interaction	There are many options available. The traditional paper-based approach of surveys has been replaced by electronic options.	P1, P2, and P3 were conducted in loci where a semi-structured interview (Mi) was administered.
Methodological Rigor	Methodological rigor refers to there being a clear decision trail of how the research was conducted.	The research process is detailed in Figure 5.7, and extrapolated in Section 5.5.4.
Results	The method of data analysis and results reporting are related to the type of questions asked.	This research made use of a qualitative approach and the analysis is detailed in Chapter Six.
Further Verification	The strength of generalisation of the results needs to be conducted.	The initial model was designed through a literature review and then refined through expert review and related to the ISO/IEC 29100 standard and PoPI Bill of 2009.
Publication	The Delphi instrument that was used for the collection of the data should be included with the research report.	The expert review process used is represented in Figure 5.7 and briefly described. It is related to the discussion in Chapter Six where the data collected from the experts is analysed.

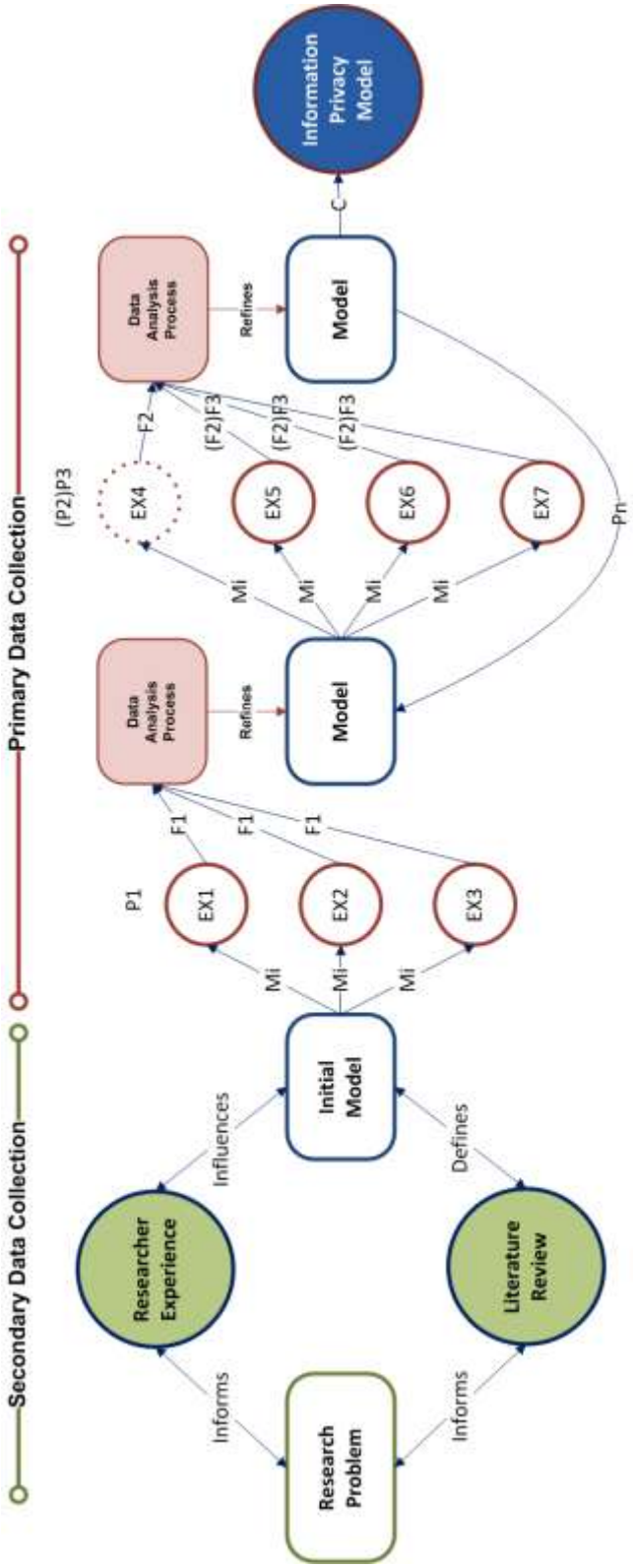


Figure 5.7: Expert Review Process followed for this research

The *literature review* done therefore assisted in defining the *initial model*. The interaction of the researcher in the creation process (*researcher experience*) required further searches to be made of the literature. The bi-directional arrows indicate the iterative literature search processes that accompanied this initial creation of the model from the identified *research problem*.

The primary data was collected by making use of the process shown in Figure 5.7, where the following notations were used:

Mi – mode of interaction is in loci (in a place) – using the interview guide
E(x) – the individual expert (reviewer/respondent) that participated in the research
P(x) – the number of the phases being conducted, where Pn refers to starting a new phase
F(x) – the collective feedback received from the experts in the phase
C – the point at which sufficient conclusions were reached

Three phases were conducted during the process of data generation. Phase 1 (P1) involved three experts (EX1, EX2, EX3) that was conducted in the same location, or *in loci* (Mi), and the associated feedback (F1). The focus of P1 was to determine the expert's opinions about privacy and to request comment on the initial model. The feedback received was analysed and used to refine the model, so that Phase 2 (P2) could be initiated. P2 was conducted with four experts (EX4, EX5, EX6, EX7) in the same location, or *in loci* (Mi), but at separate times. The feedback (F2), was analysed and used to further refine the model. The process was then repeated (Pn), such that Phase 3 (P3) was also conducted in loci (Mi) with the same experts (EX5, EX6, EX7) used in P2, but in a focus group. Expert (EX4) did not continue participating in the expert review process and therefore did not contribute to the feedback (F3). The feedback gained was then analysed and the final model changes suggested by the experts were made and the process was concluded (C). The final *Information Privacy Model* was then proposed. The analysis process, which originated from the creation and design process of the artefact (model), is discussed in Chapter Six.

Skulmoski, et al. (2007, p. 12) note the following concluding remarks on the use of the principles associated with the Delphi technique and the rich research opportunities that it provides for the information systems discipline:

- Firstly, the scope exists for the Delphi method to be aggressively and creatively adapted to a particular situation.
- Secondly, when adapting the approach, there is a need to balance validity with innovation.

The second point regarding the notion of validity once again raises the issue of how to ensure data quality, especially when utilising an interpretive paradigm and the qualitative research approach. This notion will be explored further in the next section.

5.6. Research Evaluation

It is necessary to first consider some of the concerns that positivists have regarding the shortcomings of interpretive research (Oats, 2006):

- ***Objectivity*** – the positivist will argue that there is no researcher bias, whereas interpretivist needs to be wary of their bias when conducting research.
- ***Reliability*** – the positivist will cite the repeatability of research experiments as a reason for research quality, whereas interpretivist argue that the research environment is dynamic and repetition is elusive.
- ***Internal validity*** – the positivist will rely on causality where all variables are assumed to be known, whereas interpretivist embraces the unknown and subjective nature of reality.
- ***External validity*** – the positivist strives for the goal of being able to generalise the research findings, whereas the interpretivist realises that the uniqueness of situations may make generalisation unlikely.

There are shortcomings when interpretivism is judged against positivist criteria for arriving at the truth of a given phenomenon (de Vos, et al., 2005). It can also be stated that it is evident from the work presented in this chapter that "qualitative and quantitative methods rest on different assumptions and have different purposes" (Martella, et al., 1998, p. 295). Oates (2006, p. 294) discusses the mapping of the criteria for interpretivism against those of positivism as proposed by Lincoln and Guba (1985) and represented in Table 5.6.

Table 5.6: Quality in Positivist and Interpretivist Research (Oates, 2006)

	Positivism	Interpretivism
1	Validity	Trustworthiness
2	Objectivity	Conformability
3	Reliability	Dependability
4	Internal validity	Credibility
5	External validity	Transferability

The discussion below indicates how the interpretive criteria have been applied to this research.

- Von Solms and van Niekerk (2011, p. 114) state very simply that "the research results are deemed to be trustworthy if the reader is convinced". ***For example, this research project made use of extensive literature and used the principles of the Delphi technique for the expert review process.***
- The question of researcher bias is negated by asking "do the data help confirm the general findings and lead to the implications" (de Vos, et al., 2005, p. 347), i.e. do the findings logically originate from the data and setting? ***For example, an audit trail of the data collection and analysis process was created by detailing the artefact creation and design process using an expert review process and then using the expert feedback for analysis in the next chapter.***

- As the phenomenon evolves during the research, the researcher must clearly, "account for changing conditions in the phenomenon chosen for study as well as changes in the design created by increasingly refined understandings of the setting" (de Vos, et al., 2005, p. 346). ***For example, the review of the literature and the expert review process assisted in clarifying the understanding of the context.***
- "Was the inquiry carried out in a way that ensured that the subject of the inquiry was accurately identified and described, so that the findings are credible?" (Oates, 2006, p. 294). ***For example, the Expert Review Process provided a means for the experts to review the impact of their feedback.***
- The researcher can state the theoretical parameters of the research so that other researchers can follow a similar process to arrive at the findings presented (de Vos, et al., 2005). ***For example, another researcher can consult the references used and make use of the design methodologies adopted to follow the same process, but not necessarily arrive at a similar outcome.***

Oates (2006) acknowledges that within the information systems discipline there is an increasing understanding and acceptance that interpretive research has the potential to add richness to the body of knowledge.

5.7. Conclusion

Arriving at a set of findings for a given research question is not possible without the researcher determining how they will approach the task. This is important as the researcher has to provide sufficient evidence to the reader that the research was conducted in a systematic manner. The evidence of a detailed process is even more important when adopting an interpretive approach to the research.

The interpretive paradigm was chosen at the outset for the research project and compared against the positivist and behaviour science / Design Science hybrid paradigm. Thereafter, the quantitative, qualitative and mixed conceptual frameworks to research design were discussed and the qualitative research approach chosen as the conceptual framework for this research. This led to a discussion of the strategy of inquiry that was utilised to conduct and manage the research project, namely the Design Science research guidelines.

Interviews and the principles of the Delphi technique were integrated into an expert review process, which were found to be a suitable means for detailing the research process for this research project. Finally, the credibility of interpretive research as a means of credible data collection was discussed, and criteria provided for evaluating the quality of the data.

The next chapter concerns the analysis of the data collected with the expert review process used, so that the process of creation and design of the artefact, namely, the information privacy model can be clearly articulated.

CHAPTER SIX: FINDINGS AND RECOMMENDATIONS

CHAPTER ONE:
INTRODUCTION

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

6.1. Introduction

The discussion of the literature in Chapters Two, Three, and Four provided the foundation for the development of an artefact that could be reviewed by experts. The research process followed was detailed in Chapter Five, where it was indicated that the Design Science research guidelines were followed. The guidelines informed the refinement process of the artefact that needed to be developed through the real world interaction with respondents in order to reach the aim of the study. An expert review process was used to complete the necessary interaction which comprised three iterations (phases) in order to refine the artefact. The derived artefact is an information privacy model that can be utilised in a primary health care facility to increase the awareness of privacy amongst patients and health care workers.

This chapter details how during the various phases of the expert review process primary data was collected, and then it was analysed in order to inform the refinement of the artefact. The process followed during the analysis is detailed herein and starts from the point where the interview guide detailed in Chapter Five has been administered and the responses recorded from the various experts/respondents/reviewers. The responses were solicited by making use of semi-structured open-ended questions. These responses were then coded and analysed with reference to the presented literature review in this research project and the various iterations of the model (artefact) that were refined from the initial model. The analysis was completed by using predefined themes associated with the privacy principles presented in the ISO/IEC 29100:2011(E) standard. When discussing the themes, at times direct quotes of the responses provided by a relevant reviewer are used to support a statement made, or to add clarification in the form of an example.

The review process was completed by seven experts who had expertise in the fields of privacy, information security, and/or health care. Three phases were conducted where each phase had a number of respondents and an overall focus for the phase. Phase One had three respondents and the focus was on the *aspects of privacy*. Phase Two had four respondents and the focus was on the *impact of information security on*

health care. Phase Three had three of the respondents from Phase 2 return and participate in a focus group, where the focus was the *refinement of the privacy model*.

The final model proposed for this research project is presented and takes into consideration the various suggestions and criticisms received during the expert review process followed. The ***Information Privacy Model*** is presented and explained in the final section of this chapter.

The next section will explain the analysis process followed by reviewing the various analysis steps followed, and then discuss the expert feedback received and its influence on the refinement of the final model.

6.2. Data Analysis Process

When conducting qualitative data analysis, it is necessary to follow a systematic process that indicates how the data collected was analysed (Silverman, 2011). This allows for the creation of an *'audit trail'* (Sullivan, 2012; Silverman, 2011), which can be used to structure what according to qualitative researchers has often been considered a very intuitive activity (Krauss, 2005). A qualitative research project is more likely to be considered to have independent value when using an 'audit trail', because if nothing else, the process can be replicated by another researcher (Sullivan, 2012). However, the interpretation would differ even when using a specific 'audit trail', because in interpretivism each researcher brings unique interpretations of the world to their data analysis (Silverman, 2011).

Figure 6.1 represents a high-level view of the 'audit trail' followed to analyse the data collected through the interview guide (*cf.* Section 5.5.1). There are four steps in the analysis process, which lead to the interpretation of the information for the research project. The actions completed in each step of the analysis during this research project are discussed below. Thereafter, the information collected is interpreted by using a set of identified themes. The themes used for categorising the responses were based on the privacy principles as listed in the ISO/IEC 29100:2011(E) standard, and then

discussed in terms of the artefact for this research project, namely, the information privacy model.

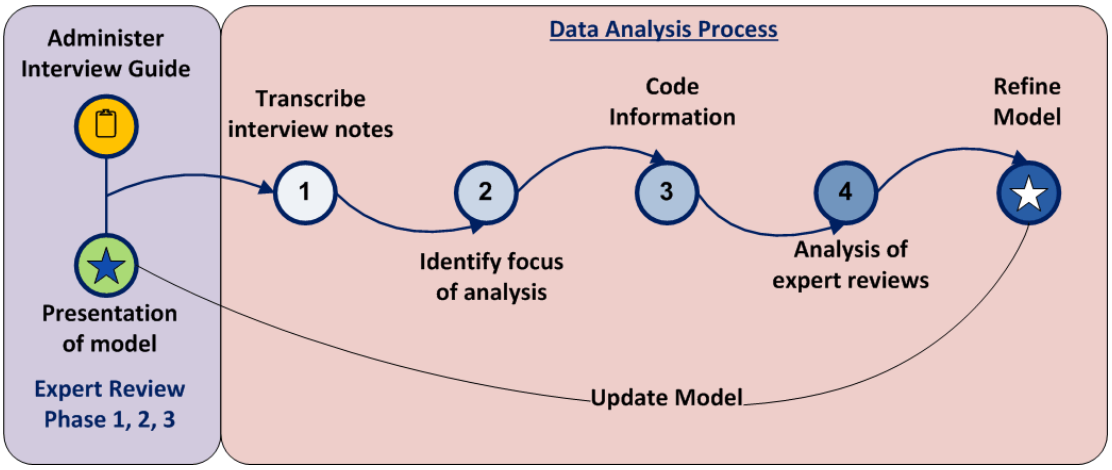


Figure 6.1: Research data analysis process (audit trail) for this study

6.2.1. Transcribe Interview Notes

The notes collected during each of the phases of the expert review process (*cf.* Figure 5.7) were transcribed and recorded in an Excel spreadsheet. The various responses provided by the experts from the semi-structured interviews were collated for analysis. Where respondents made utterances that would not be clear at the time of interpretation – the meaning was clarified with the use of an annotation recorded in [] brackets. For example, one expert constantly referred to *'manual'* records when answering the questions, which were clarified as meaning [paper-based] records. The same expert also referred to *'PCs'* interchangeably to mean either [electronic medical records], or [electronic medical record systems]. These were annotated based on the context of the answer provided.

Not all the responses recorded were directly related to the given question posed. Some responses were either tangents in the line of thought of the respondent, or related to an earlier question posed. In those instances where these deviations occurred, they were allowed to take their natural course, and all the responses

recorded. The sorting of these responses was left for later in the analysis process, i.e. step three in Figure 6.1.

6.2.2. Identify Focus of Analysis

The primary data collected for this research project was expected to serve two purposes. Firstly, to identify that the literature review conducted had covered sufficient material to address the concerns that may occur with respect to information privacy in a primary health care facility; and, secondly, to stimulate the experts cognitively on the context, so that they could actively review the artefact. It was found whilst piloting the interview guide (*cf.* Section 5.5.1) that focusing the interview questions directly on the artefact provided a poor quality response, because the respondents had not immersed themselves in the context.

The focus of the data analysis integrated the interview questions provided, and the themes that arose from the literature. These were then mapped to the data collected. The analysis write-up is ordered by the assigned codes. The codes frame the responses of the respondents in order to cognitively link to the literature done in this research project, and the various constructs of the artefact, i.e. the information privacy model.

6.2.3. Code Information

The point of coding text for data analysis is to provide meaning to the responses collected (Silverman, 2011). This was done by identifying the code(s) that could be associated with a given response. The codes that were used in this analysis were predefined and derived from the 11 privacy principles of the ISO/IEC 29100:2011(E). All 11 of the principles were assigned a code, as shown in Table 6.1. During the analysis process, these codes were assigned to the interview responses from the experts, and then it was indicated if they occurred with a given question, as shown in Table 6.2.

Table 6.1: Thematic code used

#	Theme from Privacy Principle of ISO/IEC 29100	Code
1.	Consent and choice	CC
2.	Purpose legitimacy and specification	PS
3.	Collection limitation	CL
4.	Data minimisation	DM
5.	Use, retention and disclosure limitation	UL
6.	Accuracy and quality	AQ
7.	Openness, transparency and notice	ON
8.	Individual participation and access	IA
9.	Accountability	AC
10.	Information security	IS
11.	Privacy compliance	PC

Table 6.2: Matched instance of a thematic code for responses to questions

Semi-structured interview guide question	Thematic Code
1. Can you please describe to me your general understanding of privacy law/ regulations/standards? *Protection of Personal Information (PoPI) Bill? ISO/IEC 29100 Privacy Framework Standard?*	CC, IA, PC
2. How concerned would you be about someone getting hold of your personal/ private information without your consent? Why?	CC, PS, AC, IS
3. What difference would it make if it was your medical information? Why?	PS, IS
4. How much control do you feel you should have over how your medical information is shared? Why?	CC, PS, ON
5. How would you expect patient information to be protected/ secured by those at a primary health care facility (i.e. a GPs office, hospital and clinic)?	CL, DM, ON, IA, AC, IS, PC
6. Can you please indicate who should have access to your medical information?	CC, PS, DM, UL, ON
7. What would you do to make doctors, nurses, etc. aware about keeping medical records private?	AC, IS, PC
8. What comments would you like to make about the information privacy model that has been proposed? Clarity?	CC, PS, CL, ON, IA, IS, PC

The prevalence of each thematic code from the interview responses are identified in Table 6.3. The grouping of the responses, based on their associated codes, identified *'information security'* as the most assigned theme, which occurred most often in response to questions five and seven. The theme *'accuracy and quality'* had no associated responses, but this was due to the fact that the focus was primarily on electronic medical records and not electronic health records, and those reviewed saw correcting errors as an administrative function, and not something the patient could access.

Table 6.3: Responses matched against a theme code (by prevalence) in this study

Theme Code	Matched Responses
IS	30
CC	23
AC	18
PC	11
IA	7
PS	4
UL	4
ON	4
CL	3
DM	3
AQ	0

The next sub-section will be discussed in terms of the themes identified and supported by a summary of the responses provided by the experts on that theme. The points raised with respect to the artefact are also addressed at the end of each theme.

6.2.4. Analysis of Expert Reviews

The expert review process (*cf.* Figure 5.7) indicates three phases of expert review that were conducted. The phases are discussed in relation to the literature presented in this research project and the artefact that was created. The themes identified in Table 6.1 will be used to group the various responses from the experts from Phase Two and Phase Three. The responses from the experts (EX1, EX2, and EX3) for Phase One will be dealt with in a different format as responses were only sought based on Questions 1 and 8 of the interview guide. The responses were solicited at the annual Information Security South Africa (ISSA) conference held in Johannesburg, South Africa in 2011.

6.2.4.1. Expert Review – Phase One

The first phase of expert review was derived from the feedback received at the ISSA 2011 conference. The focus was based primarily on Chapter Two of the literature contained in this research project, which is why Question 1 from the interview guide was used as a main interview question. At the time the Protection of Personal

Information (PoPI) Bill (SA Justice Dept, 2009) was not promulgated into an Act and the ISO/IEC 29100:2011(E) standard was due for release later in 2011. All three experts had seen the Bill and draft/working versions of the standard. The insights of the experts to these two pieces of privacy compliance and the impact they might have was discussed. The comments provided by the experts were generalised and not specific to the health care sector.

The experts were asked during the interview if they would be willing to make comments on the literature and model that was included in an article submitted to the ISSA 2011 conference as a research-in-progress paper (*cf.* Appendix A). The experts agreed and commented on subsequent days of the conference. The experts all felt that the discussion on privacy in the article was thorough, but felt PoPI and ISO/IEC 29100 should be included; even if in draft format. They further stated that the impact of PoPI would be significant for South Africa, and many bits of ancillary legislation will have to be aligned to this omnibus legislation on privacy. One expert **(EX3)** had this to say about PoPI and ISO/IEC 29100:2011(E):

> *"We will only begin to realise the significance of this piece of legislation once we start encountering the problems of actually complying. The Act won't tell us how to comply, but just that we must. It will be up to individual companies to figure out how to set up their ICT to comply, and I have no doubt that some companies will find loop holes without falling foul of the Act. They are already finding workarounds for the Consumer Protection Act. The standard [ISO/IEC 29100] will definitely be a step in the right direction to find out what we need to do to ensure privacy compliance, but it is not a silver bullet".*

The sentiment expressed by **(EX3)** was echoed by the other experts. When asked about the model, expert **(EX1)** felt that the model included at the end of the article was *"weak and not self-explanatory to a reader without having a thorough knowledge of privacy [legislation/regulations/standards]"*. Another expert **(EX2)** said, *"All the elements of privacy are represented, but the design of the model needs to be revisited –*

how it fits together would definitely not be clear to someone who was not confident about their knowledge of privacy".

Further criticism from an expert **(EX2)** was that the model was not an *"information privacy awareness model"*, but rather just an *"information privacy model"*. It was suggested that awareness could be an intended purpose of the model, but as the model constituted only privacy constructs there was no significance to adding the word *"awareness"*.

A concluding comment from an expert **(EX1)** during their interview session was that *"the representation of privacy as a model has a lot of potential … [especially] an explanation of how the model came about, i.e. what steps were used to derive such a model. It would also benefit the layperson who cannot figure out head or tails of legal speak"*.

The initial model presented in the research-in-progress article and to the experts was derived from a literature review of the various privacy constructs. These are detailed in the literature review that has been compiled on privacy and documented in Chapter Two. The PoPI Bill and the ISO/IEC 29100:2011(E) standard, which were not initially included in Chapter Two are added and integrated into this research project.

The experts for Phase One only made minor stylistic comments that added no further value at the time to the interim information privacy model (*cf.* Figure 6.2). They were more interested in discussing the impact of PoPI and to a lesser extent ISO/IEC 29100 and did not engage the model thoroughly. This was an issue, i.e. poor engagement of the model outside a given context, which had been highlighted during the piloting of the interview guide. The questions required of this group were very narrow in scope, so this was not seen as a negative from Phase One. The privacy insights proved invaluable in guiding the future research process.

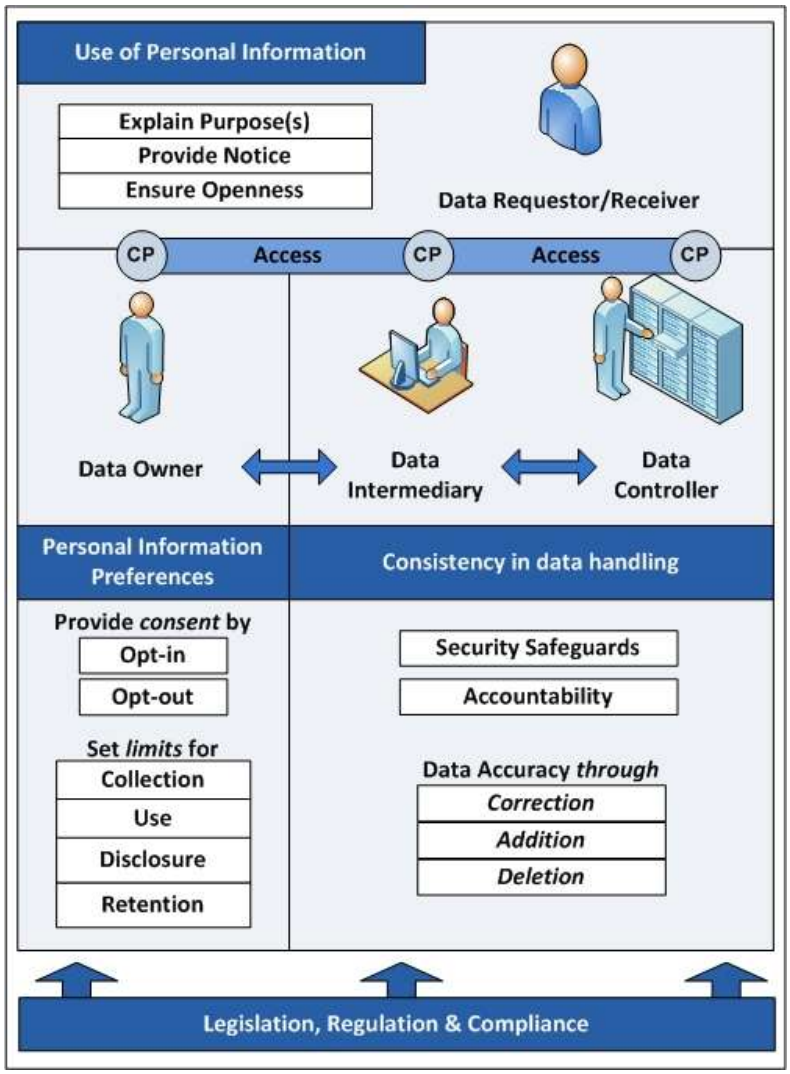


Figure 6.2: Artefact (initial information privacy model) derived from literature[24]

6.2.4.2. Expert Review – Phases Two & Three

The expert reviews conducted in phases two and three made use of the interview guide to get feedback from the experts and then link the feedback to the concepts covered in the literature and the artefact created. The initial model (Figure 6.2) was presented to the expert reviewers in Phase Two of the expert review process.

Phase Two had four experts (EX4, EX5, EX6, and EX7) who were knowledgeable about health care and information security. Their knowledge of privacy/confidentiality was

[24] Portions of this figure are represented throughout the discussion of the themes. They have not been numbered, as they are used just to highlight the area of Figure 6.2 that links to the theme.

specific to their application thereof in the health care setting and the applicable health legislation. It was not generalised knowledge as represented by EX1, EX2, and EX3 in Phase One. The intention had been to use all four experts in both phases, but one expert (EX4) did not participate in Phase Three. The aim of Phase Two was to get comments on the *impact of information security on health care*. The aim of Phase Three was to focus on the *refinement of the privacy model*.

Phase Two saw each of the experts interviewed separately, and then in Phase Three they were interviewed as a group, specifically to get consensus on the proposed information privacy model. The findings (summaries) from Phase Two with respect to the responses where shared with all the respondents, and they were asked to provide any additional points they thought might be relevant during Phase Three. There were limited responses related to the summaries, and the majority of the time was spent on refining the artefact.

The themes identified in Table 6.1 are used to focus the discussion to follow. Where a direct comment has been made about the initial model (Figure 6.2), these are included at the end of each theme discussion. Those comments regarding the model that cannot be categorised under a given theme are dealt with at the end of this section, and prior to the interpretation/explanation of the final model.

- **Theme 1: Consent and Choice (CC)**

This theme is concerned with how much restricted access/limited control an individual is willing to relinquish to another over their PII. The concerns regarding consent and choice expressed by the expert reviewers were not dissimilar from those detailed throughout the literature in this research project. One expert **(EX5)** commented that *"when you give consent, you are not sure what will happen with your information – there is an expectation of blind trust"*. The issue of trust was also raised by another expert **(EX6)** who stated *"unfortunately when consent needs to be negotiated, there is no appropriate way of determining if you can trust people"*. Chapter Three covered the element of trust as an aspect used in creating collective privacy boundaries, and

Chapter Four explored the different forms of consent that could be used when negotiating with others about how one's information would be shared.

One of the health care experts warned that PII is important for others to know, and that patients need to determine carefully what they are willing to share to receive treatment and what they would like to withhold. The following was the associated comment of said expert **(EX7)**:

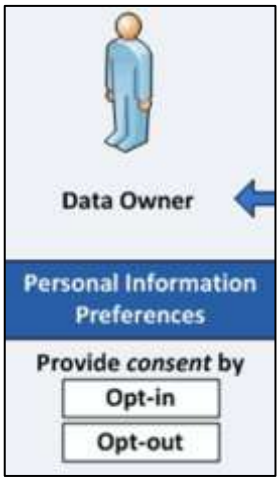
> *"You should be able to stipulate some no go areas, or certain things that are restricted from access, but generally you can't keep information secret, because a doctor or nurse may not know everything they need to and make a call about your treatment, and it's the wrong one. Trust me it [incorrect treatment based on lack of information] happens a lot more often than one would think."*

This comment ties in with the issue of control that an individual is willing to give and the experts either chose a position of complete control or semi-control. The choice of semi-control was dominant, but this could be attributed to health worker bias on the part of the experts to the fact that a patient should not hold complete control over their information as discussed in Chapter Three.

The decision regarding the level and type of consent is largely felt by the experts to revolve around the notion of implied consent. They each had differing opinions over how much control the patient had over their PII once they had entered the primary health care facility. However, all agreed that there should be specific consent for specific purposes, and that implied consent should only extend so far. As one expert **(EX5)** stated, *"the whole idea of implied consent is really only limited to certain procedures. If I want to take blood from a client who I am treating for an ailment, I may need specific consent".*

The issue with respect to consent is depicted in the initial model and the portion thereof is reproduced here for further discussion. The experts made the following general comments:

- *"Should it not be 'provide **informed** consent by'?"* ***(EX5)***
- *"There needs to be some way of showing that limits are being set. Maybe put notations on arrows [relational flows]."* ***(EX6)***
- *"Somehow the 'Data owner' needs to be shown as part of the 'Personal Information Preferences'. How would I know I am supposed to be reading the information in columns, from top to bottom?"* ***(EX5)***
- *"Maybe the safeguards have to tie in with consent."* ***(EX7)***



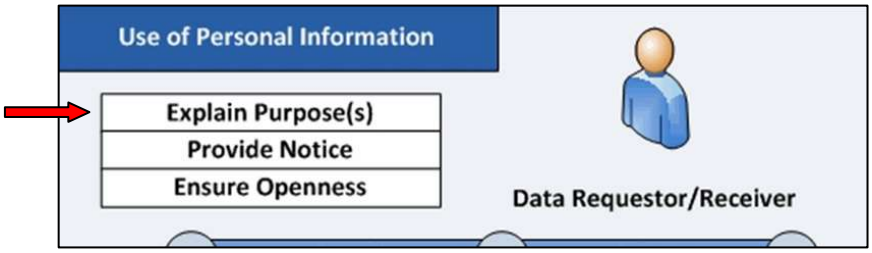
The comments raised by the experts for this theme were taken into account when the artefact was being refined. The suggestion regarding intuitive linkages through the use of relational flows was incorporated into the subsequent iterations of the artefact.

- **Theme 2: Purpose Legitimacy and Specification (PS)**

This theme focuses on ensuring that the owner of the PII is informed in an appropriate manner about how their information will be processed, and that this should occur within the ambit of the applicable law. No PII can be collected from an individual prior to explaining why it will be collected and the purpose for which it will be used.

An expert **(EX6)** stated that *"this links up with the fact that sometimes you are just expected to hand over your personal information and yet you want to know why you have to do it".* Another expert **(EX5)** provided the following example with respect to this theme: *"if I think of drawing blood – do I really know who all will have access to that medical information?"*

The only comment received by an expert **(EX6)** with respect to the model and this theme was to ask *"how do you know the information used - has been done for the intended purpose".*



It is impossible to know for certain that the information collected has been used for its intended purpose, but the Data Requestor/Receiver is shown in the artefact as being required to "Explain purpose(s)" when the "Use of personal information" is involved. This portion of the initial model will be discussed again later, so the focus of this theme is shown with the use of the red arrow in the diagram.

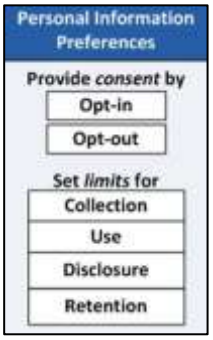
The experts suggested that the model be rearranged to indicate there is significant input from a legal perspective on the privacy compliance theme *(discussed later)*, but this suggestion has relevance here. The suggestion from an expert **(EX5)** was that the block showing *" 'Legislation, Regulation & Compliance' should flow from the top of the diagram to show that everything flows from it".*

The suggestion regarding structuring the model to indicate the intention of the label "Explain purpose(s)" being communicated to individuals prior to the collection of their information was noted. Furthermore, its link to the legal precedents resulted in the rearranging of elements in the subsequent iterations of the artefact.

- **Theme 3: Collection Limitation (CL)**

This theme is concerned with ensuring that only the PII allowed within the confines of the relevant legal precedents is collected. It also requires that PII is only collected for an intended purpose.

An expert **(EX5)** noted that *"there should be agreement amongst 3rd parties about what information will be collected".* It has been mentioned throughout the literature of this research project that a patient should expect that they will not have PII collected that will not be directly utilised for their treatment. Furthermore, the PII should not be repackaged by third parties and utilised towards another end, e.g. medical research. The law can restrict the amount of PII that needs to be collected, but by viewing this theme in relation to Theme 1 (consent and choice), it is possible to see that the patient can also influence what PII is collected about them.



The suggestions by the experts with respect to the model focused on how the limits on collection could be imposed, and it was proposed that relational arrows should be used in some manner. The point raised was similar to that of Theme 1 with respect to the model, and again showed the interrelatedness between the themes. A further suggestion by an expert **(EX6)** was that "Use of Personal Information" be changed to "Request of Personal Information for Use", and the limits linked to that title. These suggestions with respect to the order and layout of the model were noted, and included in the subsequent iterations of the model during the creation process.

- **Theme 4: Data Minimisation (DM)**

This theme is closely linked to Theme 3 and is concerned with limiting the amount of PII that gets processed through the Information and Communication Technology (ICT) systems of the organisation. The principle behind the theme stipulates how many people should have access, the restriction on the amount of PII people can access, the masking of PII as possible to avoid identifying people, and the retention of outdated/irrelevant PII.

An expert **(EX7)** made the following comment when recounting experiences of using electronic medical records at a primary health care facility – *"the patient's details [PII] are kept in a master list [database], and not recorded on the file [electronic medical*

record]. They just have a number as a reference, and all the other stuff [PII] is not visible". Another expert **(EX6)** also stated that they would be happy with their medical information to *"be shared for research purposes, as long as there was no way to identify them [data is anonymised]"*.

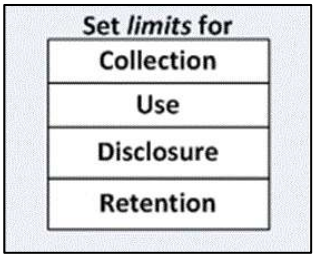
There were no specific comments related to the model with respect to this theme as its focus is the usage of the ICT to ensure the various legal and personal requirements are carried out as required. However, an expert **(EX7)** made a comment that this theme could somehow be reflected in the final model, although its omission would not be a limitation of the model. During the iterative process undertaken to finalise the model the point raised regarding the incorporation of the ICT element was kept in mind.

- **Theme 5: Use, Retention and Disclosure Limitation (UL)**

This theme is concerned with limiting how PII will be used, what will be retained (according to legal requirements and the intended purpose), and anonymising it for future use or destroying it. It is also concerned with permanently securing (through archiving) the PII, if there are legal requirements of retention.

The experts raised general comments about the manner in which medical records would be used and shared with others. One expert **(EX5)** stated that generally they did not foresee a problem where *"the primary doctor [1st doctor seen] would have authority to decide if he would allow authorisation to release records to another specialist"*. Although, another reviewer **(EX7)** cautioned that the initial purpose should still be applicable, if not, then the data should be anonymised. This was also evidenced by the earlier quote of a reviewer **(*cf.* Theme 4 – EX6)** where it was stated that it was more acceptable to share data for research purposes when it was anonymised.

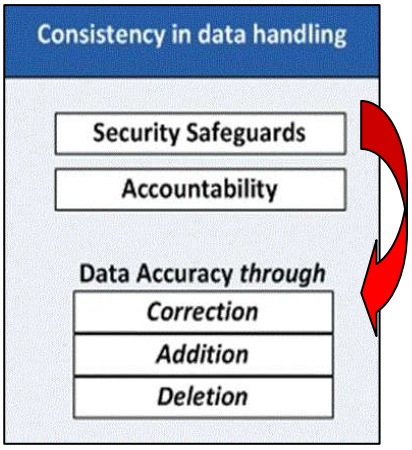
The PoPI Bill raises a number of exceptions when the PII of an individual may be used for a specific purpose without necessarily getting consent from a patient. However, there are provisos with respect to when this can be legally done according to the Bill.



The only significant comment made about this theme with respect to the model was to consider a different manner in representing the use, disclosure, and retention as shown in the image alongside. The concern was that it was not necessarily intuitive as to how they related to the other elements in the model and the various actors. The suggestion was that relational arrows could be used to depict their use and association with the relevant actors. It was further pointed out that the logical connection to the legislation element in the model also needed to be more clearly reflected.

- **Theme 6: Accuracy and Quality (AQ)**

The irony is that although this theme is probably one of the most important considerations when dealing with medical records, it was not mentioned either directly, or in relation to another theme by any of the experts during the interview questions. The risk of an incorrect treatment being administered based on incorrect or incomplete data could have a significant effect, i.e. death.

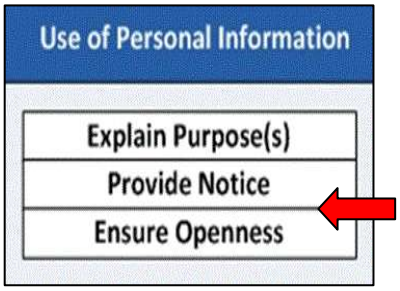


The focus of this theme is on ensuring that the PII recorded is processed correctly. It also requires validating the source of information to determine whether or not it meets the requirements of good quality data as discussed in Chapter Four. In order to ensure the quality of data, control mechanisms need to be in place to ensure that data is continuously scanned for anomalies or inconsistencies. One of the experts **(EX7)**, when discussing the security of electronic medical record systems, felt that the proximity of the "Security Safeguards" to the data accuracy elements was confusing, and it gave the impression that one might overwrite the other. This concern was noted and the layout of the model was altered, so that any potential confusion could be removed, or at best, minimised.

- **Theme 7: Openness, Transparency and Notice (ON)**

This theme is concerned with how the entity holding PII makes its policies for managing the PII known and available to the individual who owns the PII. It must be done in such a manner that it is not hidden in legalese, but makes it easy for the owners of the PII to understand the restrictions and controls associated with the processing, access, correction, and removal of their PII. The PII owner should also be kept informed of any changes that may take place with respect to how their PII will be handled.

The experts agreed that the primary health care facility needs to make it understood to the patient when their consent may be legally circumvented by health care workers by presenting this information in a clear policy, or detailed procedural manual. If a patient's medical record is accessed outside the parameters of consent and the exceptions to consent, then the patient must be notified of the breach. This notification is more easily completed if the record is electronic, as the rules can be built into the system, but if a human transgresses the rules outside the control of the system, then it is more difficult to know that a breach has occurred.



Only one expert **(EX5)** commented on the model by querying whether "Ensure openness" could not be changed to be "Ensure transparency". It was discussed that they fall within the same theme, so it could be possible that the term transparency would be more understandable than the term openness, and their meaning is similar. The suggestion with respect to the change to the model was noted, and applied to the iterations of the artefact.

- **Theme 8: Individual Participation and Access (IA)**

With this theme, one is concerned with allowing the PII owners to access and review their PII, and only theirs, unless they have authority within legislation to access the PII of another. The owners of the PII can investigate the accuracy and completeness of their PII - and amend, correct, or remove it as required. It is ultimately the responsibility of the primary health care facility in this instance to ensure that this is possible in a manner which is effective and efficient for both the PII owner and the relevant facility.

The difference in how a paper-based versus electronic medical record could be accessed by a given patient or someone else was highlighted by the reviewers. An expert **(EX7)** stated that *"providing a patient access to their file was not as easy as one would think"*. During the discussion session of Phase Three this was clarified as referring to setting up policies and procedures to allow a patient or someone at the facility to access the record. Although, expert **(EX5)** explained, *"There are often duplicate of records in paper-based health care environments. The patient's version and that kept by a specific department/doctor at a primary health care facility. From my experiences on an EMR system, it appears quite possible that a doctor can add notes to a patient's file, but the question of who owns the doctor's notes is debatable. It is also not practical for a patient to get access to an EMR. An EHR on the other hand, would definitely make access easier"*.

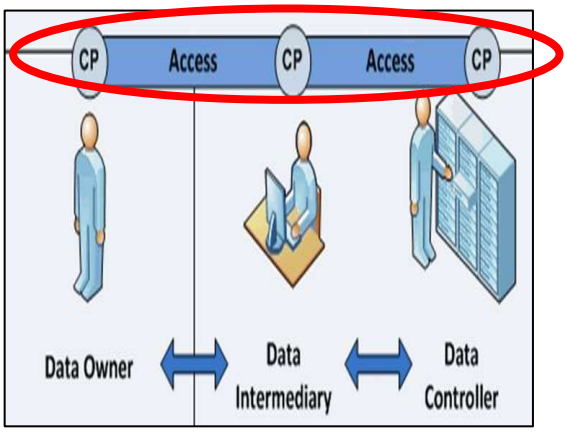
Delbanco, Walker, et al. (2012) conducted research on the use of 'open notes' for patients, where they could access their doctor's notes recorded on their EHR through the use of a web portal. The research found that:

- 77% to 87% reported that they felt in greater control when they could see the notes.
- 60% to 78% reported increased medical adherence to prescriptions.
- 26% to 36% had privacy concerns.

- 1% to 8% were not comfortable with accessing the notes.
- 20% to 42% shared their medical details with someone else.

Although the research highlighted some issues, such as: doctors changing notes already documented; taking time to compile notes; patients believing they should be able to comment on doctors' notes; a 1/3 of all patients believed they should approve doctors' notes, but there was significant resistance from doctors; and, finally 99% of the patients who participated in the research and all the doctors agreed that 'open notes' should continue (Delbanco, et al., 2012). The question then of accessibility to doctor's notes appears positive, albeit with doctors wanting to limit control by the patient to amend notes and prescribe how the notes are recorded.

In the model, the theme associated with patients being able to access their records is represented by the model portion shown. It was suggested by the experts that the section circled be replaced by relational arrows with appropriate labels. This recommendation was noted, and applied to iterations of the model refinement process.



- **Theme 9: Accountability (AC)**

The accountability theme is directly related to the duties and responsibilities that would be expected to be in existence at the primary health care facility in order to protect the processing of the PII. The various requirements are listed below and where applicable a reviewer's comment is provided. The requirements include:

- ***Documenting and communicating*** the details of privacy-related legislation as required. An expert **(EX5)** stated that it is necessary *"to start with some sort of policy of how to deal with privacy"* when attempting to get health care workers to be held accountable.

- ***Assigning a privacy champion*** to ensure that the policies are documented and communicated to all concerned parties.
- ***Ensuring 3rd parties handle PII correctly when it is transferred***, so that there is a consistent level of PII protection across zones.
- ***Providing suitable training*** to the health care workers required to access the PII within the facility. A expert **(EX6)** stated, *"I would definitely train staff, but it is not always effective. The employees need to be made aware of what they have and don't have access to. What they can and should not see about patients."*
- ***Setting up procedures*** to deal with PII owner complaints and resolution.
- ***Informing PII owners that a privacy breach has occurred*** and providing the structures to redress the breach. An expert **(EX5)** raised the issue of privacy breaches by stating, *"Provide training, but include the more practical awareness of consequences of inappropriate use or what constitutes a breach of privacy".*

When considering the model an expert **(EX6)** posed the following question, *"why are the consequences of actions not shown – are these covered in the legislation – or by a policy of the primary health care facility?"* It was discussed by the reviewers during phase three, whether it was possible to reflect the required information on the model. During this discussion, it was further raised that the "consistency in data handling" element was not easily understood. It was suggested that the "accountability" element may need to be decomposed in some manner to, at a bare minimum, mention the issue of a data breach. The comments made were considered in the final model that was being refined.

This theme of accountability also links up with the considerations for the establishment of a security culture as detailed at the end of Chapter Four.

- **Theme 10: Information Security (IS)**

The theme is concerned with ensuring that the appropriate level of information security is put in place to protect the PII throughout its life cycle. This will involve ensuring that there are controls in place to manage the PII, so that the integrity, confidentiality and availability of the PII are ensured. Furthermore, it is necessary to ensure that the PII is protected from any risks associated with access, use, modification, destruction, disclosure or loss. These must be guided by the various legal requirements for safeguarding PII.

The experts had many comments to make about issues surrounding information security, but the following two sound bites probably best highlight the careless nature of health care staff when managing patient records. Both show that unauthorised access to patient records is not that difficult in some cases, and this can be attributed to there not being adequate controls in place.

> *"A messenger delivers the blood work to all the wards from the Blood Testing Unit. This [blood work] is just contained in a sealed envelope, but the envelope is left lying around. Eventually, the envelope is opened and the patient's blood results sorted. It is often placed on the top of an open patient file and left at the patient's bedside for the doctor to review. Also, the scary thing is that it is surprisingly easy to access a patient's results from a test. All you need is the patient folder number, which is normally on the front or spine of a patient's file. Using this number, you phone the laboratory, and just say you are doctor so-and-so following up on this patient folder number. You need not even be a doctor. The labs seldom check, or even know."* **(EX5)**
>
> -  -
>
> *"I visited a friend in hospital recently, and was shocked at how relaxed the nursing staff seemed with a patient's medical records. My friend said she wasn't sure what was wrong with the woman next to her, as she was constantly weeping and it was really disturbing. A nurse came into the ward about 10 minutes before the end of visiting hours and placed the medical records of the patients on the trolleys over the foot of their beds. She then left. Nobody else had a visitor in the ward, so I stole a glance at the wailing patient's file. It was that easy, and shared the information with my friend."* **(EX6)**

The discussion amongst the reviewers during phase three further identified instances where the health care personnel circumvent controls, or simply where the controls are inadequate. An expert **(EX5)** also raised a concern that electronic medical records are often thought to be a means to solve the medical inefficiencies associated with the paper-based record, but sometimes they are inadequate for the task. The following response was recorded:

> *"So one assumes that PCs [EMR systems] will make everything safe and secure, but that is not necessarily the case. Let me give you an example … On a recent use of an EMR system, I was surprised that I was able to access all patient details from a schedule of appointments at a general workstation. My access was not restricted to my patients on the schedule, but rather I saw all their details when I accidentally clicked on the wrong patient name on the schedule. So I was allowed access through this PC [EMR system]. There was no filtering of information that was specific to the care that I was giving. Nothing was restricted. I mean, I could see the patient's entire medical history – even though it fell outside of my area of expertise. I mentioned my concern to colleagues, and they said they did not even know it was possible."* **(EX5)**

The experts' only comment specific to the model was that the element "security safeguards" needed to be more integrated into the model. This point was taken into consideration while the model was being refined.

- **Theme 11: Privacy Compliance (PC)**

This theme is concerned with whether the legal requirements with respect to privacy have been followed. The primary health care facility would need to demonstrate that they have controls in place to adequately protect PII, which policies are known, and they will need to constantly conduct risk assessments to determine if requirements for privacy compliance are being met. The various legislation and guidelines detailed at the end of Chapter Two on privacy and Chapter Three on confidentiality have reference to this theme.

The experts all indicated that they had a fair to adequate amount of knowledge about privacy in health care, and its relation to information security. They stated that health

care workers needed to be adequately trained on the principles of privacy. This comment was raised in respect to the health care worker becoming complacent in the carrying out of their privacy compliance duties and responsibilities.

The only comment regarding the model related to the design aspect mentioned earlier, i.e. the placement of the legislation element. It was felt it did not have adequate significance where it was currently placed. The experts believed it should have a more prominent role in the model.

A number of general comments were made with respect to the model that was not included in the discussion of the expert reviews with respect to the ISO/IEC 29100 standard (ISO/IEC 29100, 2011). These general comments by the reviewers are provided before the final information privacy model is presented and briefly explained.

- **Actors** – the naming of the actors on the model was not intuitive **(EX4; EX5; EX6; EX7)**. The ISO/IEC 29100 identifies four roles associated with privacy compliance namely: PII principals, PII controllers, PII processors and third parties. All these actors are represented on the initial model, but are noted as Data Owner, Data Controller, Data Intermediary and Data Requestor/Receiver, respectively. It was further suggested **(EX5; EX6; EX7)** that as the model is to be associated with the context of a primary health care facility that the actors could rather be: Patient, Clinic Administrator, Health Care Worker and Third Party Agent, respectively.
- **Structure** – the modular structure of the initial model was found to be too insular by some of the experts **(EX4; EX7)**. A number of suggestions were received with respect to changing the structure, namely: to a more flow orientated diagram **(EX5; EX6)**, that clearly shows the relational flows **(EX5)**, to a central core concept with exploding elements **(EX4)**, and finally to clearly show the core elements needed to ensure informational privacy **(EX4)**. The final point was raised **(EX7)** with respect to the processes that would differ from one primary

health care facility to the next. However, irrespective of the processes, those facilities would all need to have the required privacy elements.

The next section will discuss the proposed model that was finalised using the comments raised by the reviewers. The proposed model to be presented has undergone significant change with the various phases of the expert review process followed and the constructive comments by the reviewers both in respect to the theoretical as well as practical aspects of the final model presented.

6.3. Presentation of the Information Privacy Model

This research project made use of Design Science research guidelines for artefact development, and an expert review process was utilised to get feedback from experts on the initial model. Olivier (2004, p. 8) states that a model should capture only the essential aspects of a system or process. He further defines a model as having distinct characteristics, which are discussed in relation to the presented model (*cf.* Figure 6.3) for this research project, namely (Olivier, 2004, p. 49):

- **Comprehensiveness** – the model includes all the relevant aspects associated with the literature of the research project. It reflects the patient's ability to restrict access and the limited control that they have over how others manage their PII. It highlights the significance of boundaries when sharing PII.
- **Generality** – the model's focus is on a primary health care facility, which could be generalised to other settings. The actors are specific to this context, but could be generalised to another context or setting. There would be minor changes required, e.g. Patient, simply becomes Consumer.
- **Exactness** – this model is specific to the health care context, but includes all the elements associated with the accepted privacy principles. It is further aligned to the ISO/IEC 29100 standard by

incorporating all the principles detailed therein through their use as themes during the data analysis process. It is also related to the principles included in the PoPI Bill.

- **Clarity** – the model has been colour coded in places to provide ease of interpretation to the reader. The reviewer's original criticism of the initial model in Phase One was that it was not intuitive enough. The relational flows detailed in this model provide an easy process flow that can be followed with minimal narrative in support.

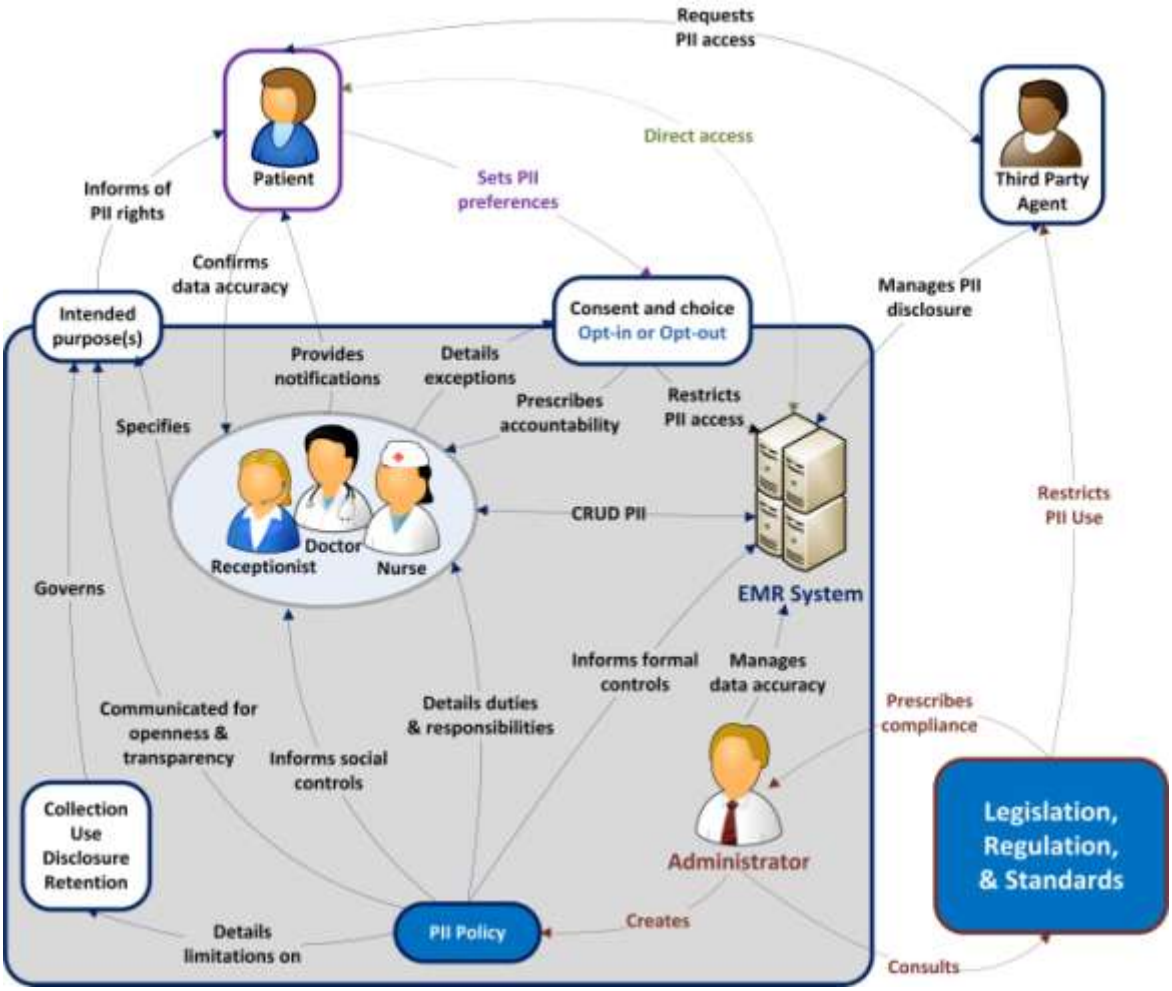


Figure 6.3: Proposed Information Privacy Model developed during this study

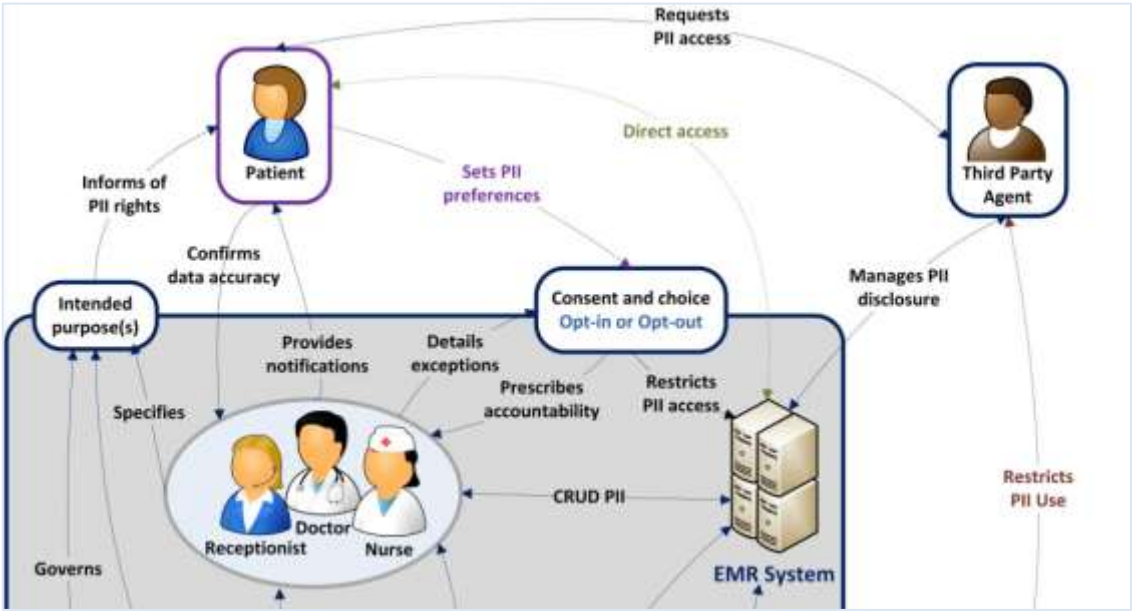
The data analysis covered in the previous section listed the findings from the research project. This section will now detail the recommendations for this research project

with respect to the information privacy model that was developed. The principles detailed in the PoPI Bill (*cf.* Table 2.4) (SA Justice Dept, 2009) are used throughout this section. They are used to explain the model, and thereafter how it addresses the research question posed, i.e. ***How can the awareness of concerns surrounding privacy and confidentiality influence the accessibility to electronic medical records at a primary health care facility?***

For the purposes of explaining the model, it has been divided in half. The lower half will be discussed first as this is the starting point for the entire compliance process.

The **Administrator** actor of the primary health care facility needs to consult the relevant legislation *(e.g. PoPI)*, regulation *(e.g. the HPCSA guidelines on the confidentiality of patient information)*, and standard *(e.g. ISO/IEC 29100 and ISO/IEC 27799)* in order to determine what is required for the facility to comply. Once the requirements with respect to compliance are understood, the **Administrator** actor (or a designate) creates a policy that details how the personally identifiable information (PII) of the **Patient** actor is to be protected whilst it is being processed in the primary health care facility. The **PII Policy** will detail the limitations with respect to the ***collection***, ***use***, ***disclosure***, and ***retention*** of PII. The policy in order to meet with legal compliance needs to be communicated in a manner that is free of legal jargon, and could be understood by a "reasonable man". This would detail how the policy will be implemented and the recourse that the **Patient** actor has if something happens to their PII. This would correspond to the PoPI principle of ***openness***. The policy to meet compliance needs to indicate what social controls (e.g. the cultivation of a security

culture) will be put in place in order to ensure that the **Health Care Worker (Receptionist, Doctor and Nurse)** actors are aware of their duties and responsibilities. These duties and responsibilities are detailed in the **PII Policy** and indicate where and when a **Health Care Worker** actor is accountable with respect to compliance. These requirements with respect to the **Health Care Worker** actor relate to the PoPI principle on ***accountability***. Finally, the policy needs to be converted into formal controls (as discussed in Chapter Three) that are developed by the information security specialists (a designate of the **Administrator** actor) to ensure that the necessary PoPI principle on ***security safeguards*** are in place with respect to managing the PII of the **Patient** actor. The policy, will also detail how the relevant access controls would be assigned and the duties and responsibilities that would be associated with them. Additionally, the limitations with respect to the collection, use, disclosure, and retention of the PII will need to be detailed into the **EMR system**. Finally, it is the responsibility of the **Administrator** actor according to the PoPI principle on ***information quality*** to ensure that there is accuracy in the management of the PII. The importance of the integrity of data was discussed in Chapter Four of the literature.



The **EMR system** in the image above has been set up by the information systems specialists (**Administrator** actor designate) based on the **PII Policy**, which in turn was created in order to meet various compliance requirements. The **Health Care Worker**

actors are detailed in the image as the **Receptionist**, the **Doctor**, and the **Nurse** actors. Each of these actors would have different access restrictions with respect to being able to **c**reate, **r**ead, **u**pdate, and **d**elete PII. This again links with the PoPI principle on ***accountability***. These access restrictions are shown on the bi-directional arrow 'CRUD PII'.

The **EMR system** will also restrict the PII that a **Third Party Agent** actor (e.g. a medical aid) is allowed to request. There are also legal restrictions that govern the use of PII, and these would be detailed on the **EMR system** through the **PII Policy**. This links to the PoPI principle of ***further processing limitation***, where data collected for a specific purpose cannot be repackaged and used for another purpose without the consent of the data owner (**Patient** actor). The **Third Party Agent** actor would also need to directly comply with the restrictions for PII use as detailed in the relevant legislation, regulation, and/or standard. The **Patient** actor has the power to *restrict access* to their PII and thus retain *limited control* over their PII. This choice made by the **Patient** actor would be recorded on the **EMR system** and will inform future disclosures to **Third Party Agent** actors. The **Third Party Agent** actor has the choice to contact the **Patient** actor directly to request that they amend their preferences with respect to PII, e.g. if doing medical research. However, there are provisos in legislation relevant to the notion of 'public good'[25] and 'unreasonable expectation of notice'[26], that can circumvent this action on the part of the **Third Party Agent** actor.

The **Patient** actor has a significant right over restricting their privacy from access, but is only protected with respect to the relevant compliance requirements when interacting with the primary health care provider. Legal compliance, e.g. the PoPI principle – ***purpose specification***, is very specific about the fact that a data owner (the **Patient** actor) needs to be informed about why their PII is being collected *(collection)*, how it

[25] The PoPI Bill makes provision for the overriding of consent, where the intended action will be in the interest of the public good.

[26] The PoPI Bill and the various 'medical' Acts in South Africa prescribe that a reasonably documented (e.g. a newspaper advert, personal letter, mobile message) attempt needs to have been made in order to contact the owner of the PII to request their consent. However, where this is not logistically possible (a grey area) or no response is forthcoming the notion of implied consent is assumed to be active.

will be used *(use)*, who it may be shared with *(disclosure)*, and for how long it will be retained *(retention)*. The responsibility falls on the **Health Care Worker** actor to specify for the **Patient** actor how their PII will be collected, used, disclosed, and retained. However, the **Health Care Worker** actor can only inform the **Patient** actor based on the thoroughness of their understanding of the compliance requirements in the PII policy that are adequately communicated to them. The adage, "a little knowledge is a dangerous thing" seems appropriate for how the **Health Care Worker** actor would interact with the **Patient** actor if they were not well informed about the implications with respect to privacy and confidentiality.

The **Patient** actor sets their PII preferences with respect to **consent and choice** by defining who can access what information when, where, and how. This will largely be influenced by how much trust (*cf.* Chapter Three) the **Patient** actor has in the **Health Care Workers** and the **EMR system**. The **Patient** actors' choices regarding consent are recorded into the **EMR system** based on their restricted rights to accessing their PII. Only information specifically required from the patient to allow treatment should be collected and no other. This issue of consent has been covered in Chapters Three and Four, and is associated with the PoPI principle, ***processing limitation***. Once the **Patient** actor has decided on their PII preference settings then the information is communicated to the **Health Care Worker** actors based on their prescribed accountability with respect to the **Patient** actors' consent requirements. The **Health Care Worker** actors will also inform the **Patient** actors of any exceptions that they may need to be aware of where their consent preferences may not apply. This would be based on some legal precedent where compliance can still be maintained in the presence of the exceptions.

The PoPI principle, ***individual participation*** – states that the **Patient** actor has the right to access their personal information and correct it as required. The model shows two avenues of interaction with respect to participation. One is through the **Health Care Worker** agents by getting them to allow access to and correction of a patient's record. An alternative is also shown in the model where the **Patient** actor can access their electronic medical records at the primary health care facility through a web portal or

similar method directly into the **EMR system**. This link is tentative on the technology available and is shown as a dashed line. Irrespective of the means of participation of the **Patient** actor, it is important that the **Health Care Worker** actors detail the procedures for how, when, and where a **Patient** actor may gain access to these records.

The final item on the information privacy model that needs consideration is where the **Health Care Worker** actor provides notification to the actor with respect to a breach that has occurred, or an anomaly that has been encountered in their medical records. This links with the PoPI principle of ***security safeguards***.

In summary, it can be stated that the research question for this research project, i.e. ***How can the awareness of concerns surrounding privacy and confidentiality influence the accessibility to electronic medical records at a primary health care facility?*** – has been addressed. The model recommends how the actors at the primary health care facility play an integral role in ensuring that the patient's rights and confidentiality are met. This is done by interpreting the compliance requirements and sharing these with the patient in a manner that can be understood by a 'reasonable man'. However, this can only be accomplished by raising the awareness of those employed at the primary health care facility with respect to their duties and responsibilities.

6.4. Conclusion

The primary data was analysed in this chapter following a sequence of events that constituted a clear and logical audit trail. The data collected (interview responses) in each of the three phases of the expert review conducted within the expert review process used were coded for easy use. The codes were derived from the principles of the ISO/IEC 29100:2011(E) standard which details how to deal with risk associated with privacy within a privacy framework. These codes were mapped against the semi-structured questions of the interview guide and detailed that information security arises as the highest ranking theme, followed by compliance.

The responses received from the three respondents (EX1, EX2, EX3) in Phase One were dealt with separately, as these respondents' answers were focused on questions 1 (dealing with privacy compliance) and 8 (commenting on the model). The comments regarding the legislation and standard under discussion were then incorporated into the literature review to address perceived gaps in knowledge, and used to refine later iterations of the artefact (model).

The responses from the respondents (EX4, EX5, EX6, EX7) were included in the discussion on the outcome of Phases Two and Three. The data was discussed cumulatively for ease of analysis. The primary data was discussed by using the principles of the ISO/IEC 29100:2011(E) as the themes for discussion. Each of the themes was explained and then relevant responses from those received from respondents were added to punctuate a point. On occasion sound bites (extended quotes) were used to provide further insight into the theme. These findings assisted in determining the expected outcome of this research project, namely, the information privacy model. This was accomplished by merging the themes identified in both the primary and secondary data.

The comments of the respondents on the artefact (model) were collated through an iterative process, which informed the refinement and presentation of the final information privacy model for primacy health care facilities. The model was then explained as a means to recommend a holistic view of increasing awareness amongst the actors interacting with each other in the primary health care setting. It further highlights the importance of using the necessary compliance requirements as the starting point for establishing formal and social controls.

The chapter ends by detailing how the original research question can be addressed by the information privacy model for primary health care facilities. A description of the process followed throughout this research project is summarised in the next chapter.

CHAPTER SEVEN: CONCLUSION

CHAPTER ONE:
INTRODUCTION

LITERATURE REVIEW

CHAPTER TWO:
PRIVACY – *THE RIGHT TO RESTRICT ACCESS TO PERSONAL INFORMATION*

CHAPTER THREE:
CONFIDENTIALITY & TRUST – *CONTROL OF THE COLLECTIVE PRIVACY BOUNDARY*

CHAPTER FOUR:
ACCESSING THE ELECTRONIC MEDICAL RECORD (EMR)

METHODOLOGY, FINDINGS AND RECOMMENDATIONS

CHAPTER FIVE:
RESEARCH METHODOLOGY

CHAPTER SIX:
FINDINGS AND RECOMMENDATIONS

CHAPTER SEVEN:
CONCLUSION

7.1. Overview
7.2. Theoretical Focus and the Literature
7.3. Objective of the Study
7.4. Research Methodology
7.5. Discussion
7.6. Future Research
7.7. Concluding Remarks

7.1. Overview

The findings and recommendations discussed in Chapter Six detailed how the analysis process was followed to refine the proposed artefact for this research study, i.e. the proposed *Information Privacy Model*. The process to develop the model involved the use of secondary and primary data. The primary data was sourced through experts using an expert review process, which allowed for improved credibility with respect to the findings of this study.

In order to provide a description of how the research project arrived at the proposed model, this study is summarised and concluded in this chapter. *Firstly*, a discussion of the literature presented in the study will be provided with direct reference to the underlying theories used for the theoretical focus of this study, namely: the Communication Privacy Management (CPM) Theory (Petronio & Reierson, 2009; Petronio, 2002), the Restricted Access Theory, the Control Theory, and the Restricted Access/Limited Control (RALC) Theory (Tavani, 2008). *Secondly*, the research problem leading to the research question and sub-questions are all restated with respect to what was discussed in each chapter to address the research sub-questions. *Thirdly*, the research methodology followed to direct the data collection and analysis process in this research project is detailed. *Fourthly*, a general discussion on the research objective is presented. *Fifthly*, the limitations of the research project are considered, as well as future areas of research. *Finally*, concluding remarks are presented.

7.2. Theoretical Focus and the Literature

The literature in this study focused primarily on the philosophical constructs of privacy and confidentiality. Trust was discussed as an integral part of the establishment of confidentiality. Linked to these philosophical constructs are the associated considerations for access and control. They are intrinsically tied to the amount of information an individual is willing to disclose to another, or keep private. These various topics have been discussed throughout the literature with reference to how

the electronic medical record (EMR) of the patient is managed at a primary health care facility. They will briefly be summarised with respect to the underlying theoretical focus inherent in the discussion throughout the study.

The CPM Theory presented with five core principles that was part of the underlying premises of the research project. Intertwined with these premises were the Restricted Access Theory, the Control Theory, and the RALC Theory. In Chapter One of this research project, the CPM Theory was mapped to each of the literature chapters (*cf.* Table 1.1). Each of the principles and theories highlighted (cf. Section 1.6) are discussed within the context of the relevant chapter. Chapter Two focused on ***privacy***, Chapter Three on ***confidentiality*** and trust, and, finally, Chapter Four on ***accessibility***.

Privacy is the common theme that runs throughout the research project, as it is the underlying phenomenon, which drives an individual to act in a certain manner. This arises from an individual's expectation that they have ownership and control over their private information. Westin (1967) states that individuals have control over how much information they are willing to share, whether the choice is to withdraw or participate in society. He terms this control over individual information, *informational privacy*, or more commonly termed as information privacy.

When individuals decide to participate in society, they need to negotiate how they will limit and protect their communications with others (Nippert-Eng, 2010). Petronio (2002) proposed the CPM Theory to deal with the protection of private communication. She states that the ownership and control of privacy is associated with an individual's rights and obligations (Petronio, 2002). These rights and obligations are affected by an individual's privacy boundaries (Petronio, 2002), zones of privacy interactions (Tavani, 2008), or contextual integrity (Nissenbaum, 2010). Individuals create these privacy boundaries in order to restrict access to their personal information. This is the underlying principle of the Restricted Access Theory, insofar as individuals have the right to decide what will be kept private, and shared with others (Nippert-Eng, 2010; Tavani, 2008). From a health care perspective this would involve an individual making a decision about how much personally identifiable information

(PII) they are willing to share with health practitioners and/or 3rd party agents (Appari & Johnson, 2010).

However, the various discussions on privacy throughout Chapter Two detailed that individuals have a greater likelihood of sharing private information if they accept that some control will be exercised over protecting their information privacy. To this end, legislation, regulation, and standards are used to dictate the compliance requirements for the ownership and management of the PII of an individual. The requirements for compliance are detailed in the sets of principles included in the relevant legislation, regulation, and standards. The privacy principles included in the Protection of Personal Information (PoPI) Bill of 2009 (SA Justice Dept, 2009) and the ISO/IEC 29100:2011(E) privacy standard are introduced in this study and used during the data analysis process.

Individuals, according to the second principle of the CPM Theory, make decisions about whether to share their private information based on their personal privacy rules. These can be influenced by the context (primary health care facility) and risk/benefit ratio associated with sharing the private information, i.e. from a health care perspective the risk chosen can affect the degree of received medical treatment. However, a major concern is that not only does the individual wanting to share the information have a set of privacy rules, but the confidant receiving the information will apply either their own privacy rules, or what they perceive to be those of the individual sharing the information. This raises the concern of the level of trust one individual has in another as to whether they will complete a set of actions as expected. It also determines whether a confidential relationship will be established between two parties.

Tavani (2008) states that the underlying principle of the Control Theory is that an individual's privacy is directly linked to the amount of control that they can exercise over their PII. This is echoed in principles two and three of the CPM Theory with respect to sharing information with others.

Individuals need to negotiate the boundaries of confidential relationships by determining the level of control they desire. This will be guided by their choices with respect to consent, i.e. how their PII can be accessed and used. Individuals therefore have a choice in determining how their information will be shared. However, the level of control required is directly proportional to the expected accountability assigned to the given confidant who has access to the PII.

Compliance can be achieved through formal and/or social controls, where guidelines are provided on how primary health care facilities should deal with confidential information and patient PII. These guidelines are detailed in the Caldicott Principles (Keyser & Dainty, 2005) and the HPCSA guidelines for confidentiality (HPCSA, 2007).

The health care context of this study requires that the electronic medical record of the patient be shared with those who have the relevant authority in order to initiate medical treatment. The patient can have complete control over their medical records under ideal situations, but this can lead to problems associated with accessibility. If the patient decides to place excessive restrictions on the access to their medical record, it would require continuous notifications for consent to access the record. It then makes it increasingly difficult to treat that patient. Therefore, if the patient has complete control over the record it could mean that others may not have access to it when needed.

The RALC Theory has the underlying principle that restricted access is associated with the concept of privacy, and that the management of privacy is achieved through a system of limited control. The individual/patient would therefore have control of a given situation, or in a given context based on the consent, they had provided. The consent they had provided would give them that perceived control over the situation. The CPM Theory principles four and five state that mutually agreeable boundaries can be agreed upon, but it is also possible that those boundaries can become turbulent (Petronio & Reierson, 2009) or threatened. For example, a health care worker releases information to a third party agent without the consent of the patient, either intentionally or unintentionally.

The privacy concerns associated with accessibility were detailed in Chapter Four. It was proposed that the breaches in the relationships/boundaries could be avoided by ensuring that the patient is aware of their rights and limitations with respect to providing consent. The health care workers need to be aware of their impact as confidant with respect to maintaining the privacy of the patient. This can be achieved through the communication of the requirements for maintaining compliance through social controls, such as awareness programmes where it is possible to work towards improved compliance with respect to privacy concerns.

The four theories presented for discussion in this section have been related to the literature review by explaining that people have different privacy rules when considering the ownership/restricted access and control of PII. The next section discusses the research questions and the literature that was presented to address the relevant sub-question.

7.3. Objective of the Study

The primary objective of this research project was the development of an information privacy model for application within the context of a primary health care facility. The proposed model is expected to residually assist in raising awareness of the privacy compliance requirements that need to be considered while interacting with patients and their PII. Furthermore, the proposed model does not prescribe how PII should be managed practically, but rather presents a holistic view of the constructs of privacy in a manner free of verbose legal and philosophical jargon.

The model was derived by investigating the following research question:

How can the awareness of concerns surrounding privacy and confidentiality influence the accessibility to electronic medical records at a primary health care facility?

This research question was investigated by addressing three sub-questions, which were discussed in the relevant chapters as indicated below:

Q1: What are the constructs and legal implications of information privacy?

Chapter Two provided a discussion of the nature of privacy by providing a definition of privacy and detailing the building blocks of privacy legislation. Thereafter, a detailed discussion of informational privacy was undertaken by introducing Westin's (1967) various constructs that form part of informational privacy. These explain how individuals exercise their perceived control over their private information. To further understand the nature of information privacy, the concept of PII was discussed in order to gain a better understanding of what it entails. The PoPI Bill of 2009 was used to provide examples of the PII. An example of the typical life cycle of PII, and how it might flow through an organisation was discussed. Thereafter, the foundational elements of privacy legislation, namely the FIPs were provided in order to enter the discussion on the various types of privacy legislation available. A summary of the privacy constructs typically found in legislation were included in the chapter discussion. Finally, the PoPI Bill and the ISO/IEC 29100:2011(E) standard were introduced.

Q2: What confidentiality considerations exist with respect to the patient-health care practitioner interaction?

Chapter Three discussed the nature of confidentiality and detailed how collective privacy boundaries are established between the patient and the health care practitioner. The various constraints on the maintenance of confidentiality were discussed including the fact that the relationship between the patient and the health care practitioner becomes more difficult to maintain the further it gets from the primary point of contact. The expectations of trust were discussed as an important determinant of the level of confidence the patient is willing to place in the health practitioner. This is strengthened or weakened by the level of control that is visible to the patient when establishing the relationship. The controls (either formal or social) in existence in the primary care facility are expected to provide a greater level of

predictability of the actions of those interacting with the electronic medical record. However, violations can occur, so it is necessary to put in place regulations to guide the actions of those in the primary health care setting. Two regulations in the form of guidelines to be followed are provided, namely: the Caldicott Principles (UK) and the HPCSA Guidelines for Confidentiality (SA). Although one is from the UK, and the other SA – there are similarities in how health care practitioners are expected to conduct themselves when interacting with patients and the PII. This is evident when reviewing the guidelines side-by-side.

Q3: What factors affect the accessibility of electronic medical records in a primary health care facility?

Chapter Four discussed the concern for information privacy (CFIP) that includes the collection of information, information quality due to errors, the unauthorised access to information, and the secondary uses of information. The principles detailed in the PoPI Bill (SA Justice Dept, 2009) and the ISO/IEC 29100:2011(E) standard provides details of the actions that should be followed to avoid the CFIP manifesting. The Socio-Technical Theory (Bostrom & Heinen, 1977) was introduced through a discussion of the technical and environmental perspective of health care. The benefits that could be derived from the implementation of an electronic medical record system were detailed. This followed a discussion of the social perspectives of health care by considering three of the CFIP, namely: collecting patient information, errors in patient information, and unauthorised access to patient information. The discussion highlighted the threat that individuals with limited understanding of the compliance considerations and information security can pose to the primary health care facility and the information asset (EMR). It was proposed that the cultivation of a security culture based on the OECD guidelines for securing network systems (OECD, 2002) could be accomplished by ensuring that awareness of compliance issues are adopted.

The presented literature for each sub-question allowed for the answering of the main research question for this study. This was further accomplished by utilising the research methodology detailed in the next section.

7.4. Research Methodology

Chapter Five detailed the research methods that were followed. The nature of paradigms was discussed, and the interpretivist paradigm was justified as the focus for this research project due to the subjective nature of the primary phenomenon in the study, namely, privacy. Given the justification for the use of an interpretivist paradigm, a qualitative stance was taken. This allowed for semi-structured interviews to be used, which were informed by an interview guide. The interview guide was developed from the literature review and questions were sorted into topics for easier interpretation during data analysis.

The interviews were conducted with seven respondents through the use of an expert review process, which was based on the principles of the Delphi technique. Part of the process of the expert review process involved the respondents making comments on a developed artefact for this research study. The process consisted of three phases of review. Phases One and Two were conducted as individual semi-structured interviews and Phase Three were conducted as a semi-structured focus group. Three of the participants from Phase Two were involved in Phase Three and discussed the summaries of responses from Phase Two. Clarification was provided where required by the experts on the primary data already collected in Phase Two.

The Design Science research guidelines for artefact development were used in order to derive the final model, i.e. the information privacy model. This involved the aforementioned respondents, who are experts in one or more of the fields of health care, information security, and privacy; commenting on the artefact. The experts provided feedback on the interim model, which informed further iterations.

The relevance for the use of the Design Science research guidelines are detailed in Chapter Five, but primarily their use was considered an effective and efficient means to develop the artefact (model). The adoption of the Design Science research

approach also lent itself to the iterative process followed with the experts to assist in determining the proposed information privacy model for this research project.

The next section will provide a discussion of study conducted and how the main objective of the research was realised.

7.5. Discussion

This research project completed a literature review of secondary data that would lead to an increased understanding of the presented problem, i.e. a lack of clarity with respect to privacy compliance associated with electronic medical records in health care. The literature review considered the philosophical discussion of privacy from a multi-disciplinary approach that explored the fields of health care, information systems, law, management, psychology, and sociology. The commonality across fields always led back to the same theme, i.e. the individual needs to make the choice to keep their information private or share it. Increasingly this main theme was noticed in articles covering areas of consumer behaviour and social media.

The nature of confidentiality was researched to determine if it was or was not related to privacy. There is a belief amongst some information security specialists that privacy is not a core aspect of information security. From the literature, it was apparent that this was largely dependent on the individual. The concept of privacy or an individual's perspective of privacy determines their interactions with others and with artefacts in their environment. Intrinsically linked to this is how privacy would be managed. This involves considering how individuals restrict access and how organisations establish the controls to satisfy the privacy appetite of the individual. This notion of an individual's privacy appetite was covered in Chapter Two and Three of the literature discussion.

The literature further identified that if individuals, whether the patient or health care worker in the context of this study, are not informed about the compliance requirements they make choices or act in a manner that may have negative

consequences. This observation became evident in Chapter Four when the accessibility of electronic medical records was discussed. The ignorance, due to lack of understanding of the compliance requirements, or information security practices in general, was highlighted in the examples cited from the Ponemon Institute study (Ponemon Institute, 2012) with respect to the loss of private data.

The research process moved from the literature review, to the collection of the data, to the analysis, and finally the interpretation of the information privacy model highlighted the increased need to raise awareness of privacy, and especially the compliance thereof. It is believed the aim of this research project has been achieved, i.e. the development of an information privacy model for primary health care facilities to aid in raising awareness of compliance requirements.

7.6. Future Research

This research project focused on the development of a graphical representation of the various constructs required within privacy. The model should be further tested in the running of awareness programmes to determine its suitability for those unfamiliar with the various privacy constructs associated with compliance requirements. The model could also be generalised to other contexts to determine if the main elements thereof can be generalised elsewhere.

From the literature review conducted it was evident that much research still needs to be conducted on the processes associated with the implementation and adoption of information technology (IT) to determine if privacy-by-design is being applied, i.e. is privacy compliance there from the beginning or an add-on after the fact. It was also evident that privacy compliance is the underlying driver for information security, and privacy management through the use of various formal and social controls needs to be further explored. A further area of research could entail the considerations and practicality of the application of the privacy compliance requirements with respect to the effect these would have on effectiveness and efficiency within primary health care facilities, or any other context for that matter.

7.7. Concluding Remarks

This study sought to provide a means to understand the various compliance issues associated with privacy, so that their application within the domain of information security could be aided. The value of the study is insofar as the various constructs of privacy have been graphically represented in a manner that could stimulate thought, as to how compliance can be built into the various information systems involved in the delivery of not only patient treatment, but other services as well.

REFERENCES

Agrawal, R. & Johnson, C., 2007. Securing electronic health records without impeding the flow of information. *Int'l Journal of Medical Informatics,* Volume 76, pp. 471-479.

Ahmad, A., Guy, G. G. & Wasana, B., 2011. *Developing an IS-Impact Decision Tool: A literature based Design Science Roadmap.* Helsinki, ECIS 2011.

Angst, C. M. & Agarwal, R., 2009. Adoption of Electronic Health Records in the Presence of Privacy Concerns: Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly,* June, 33(2), pp. 339-370.

Anon., 2008. *Ebers Papyrus.* [Online]
Available at: http://www.newworldencyclopedia.org/entry/Ebers_Papyrus
[Accessed 2 4 2012].

Anon., n.d. *The Hippocratic Oath.* [Online]
Available at: http://www.hpcsa.co.za/hpcsa/default.aspx?id=275
[Accessed 2 April 2009].

Appari, A. & Johnson, M. E., 2010. Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management,* 6(4), pp. 279-314.

Avgerou, C., 2000. Information Systems: what sort of science is it?. *Omega - International Journal of Management Science,* Volume 28, pp. 567-579.

Banks, D. L., 2006. The Health Insurance Portability and Accountability Act: Does it Live Up to the Promise?. *Journal of Medical Systems,* 30(1), pp. 45-50.

Barth, A., 2008. *Design and Analysis of Privacy Policies,* Proquest.

Bennett, C. J. & Raab, C. D., 2006. *The Governance of Privacy - Policy Instruments in Global Perspective.* Cambridge(Massachusetts): Massachusetts Institute of Technology (MIT) Press.

Bloustein, E. J., 1964. Privacy as an aspect of human dignity: an answer to Dean Prosser. In: F. D. Schoeman, ed. *Philosophical Dimensions of Privacy: An Anthology (2007).* Cambridge: Cambridge University Press, pp. 156-202.

Blumberg, B., Cooper, D. R. & Schindler, P. S., 2008. *Business Research Methods.* 2 ed. Maidenhead: McGraw-Hill Higher Education.

Bostrom, R. P. & Heinen, J. S., 1977. MIS problems and failures: a socio-technical perspective. *MIS Quarterly,* 11(3), pp. 17-32.

Carr, N. G., 2004. *Does IT Matter?.* Boston, Mass.: Harvard Business School Press.

Choi, Y. B., Capitan, K. E., Krause, J. S. & Streeper, M. M., 2006. Challenges Associated with Privacy in the Health Care Industry: Implementation of HIPAA and the Security Rules. *Journal of Medical Systems,* 30(1), pp. 57-64.

Ciampa, M., 2010. *Security Awareness: Applying practical security in your world.* 3 ed. Boston: Course Technology.

Corliss, M., 2010. *The Use of Information: How new technology is changing discussions of privacy.* Ann Arbor(MI): UMI Dissertation Publishing.

Creswell, J. W., 2009. *Research Design in Qualitative, Quantitative and Mixed Methods Approaches.* 3 ed. London: Sage.

Crompton, M., 2003. *Biometrics and Privacy - The End of The World as We Know It or The White Knight of Privacy?.* [Online]
Available at:
http://www.privacy.gov.au/materials/types/download/8518/6407
[Accessed 20 September 2010].

da Veiga, A. & Hari, T., 2011. *Revealing privacy in South Africa: What you need to know,* Johannesburg: Information Security Group of Africa: Privacy (SIG).

Damschroder, L. J., Pritts, J. L, Neblo, M. A., Kalarickal, R. J., Creswell, J. W., Hayward, R. A., 2007. Patients, privacy and trust: Patients' willingness to allow researchers to access their medical records. *Social Science and Medicine,* Volume 64, pp. 223-235.

Das, T. K. & Teng, B., 1998. Between Trust and Control: developing confidence in partner cooperation in alliances. *Academy of Management Review,* 23(3), pp. 491-512.

de Vos, A. S., Strydom, H., Fouché, C. B. & Delport, C. S., 2005. *Research at Grass Roots for the Social Sciences and Human Service Professions.* 3 ed. Pretoria: Van Schaik Publishers.

Delbanco, T., Walker, J., Bell, S. K., Darer, J. D., Elmore, J. G.; Farag, N., Feldman, H. J., Mejilla, R., Ngo, L., Ralston, J. D., Ross, S. E., Trivedi, N., Vodicka, E., & Leveille, S. G., 2012. Inviting Patients to Read Their Doctors' Notes: A Quasi-experimental Study and a Look Ahead. *Annals of Internal Medicine,* Volume 157, pp. 461-470.

Deshefy-Longhi, T., Dixon, J. K., Olsen, D. & Grey, M., 2004. Privacy and Confidentiality in Primary Care: views of advanced practice nurses and their patients. *Nursing Ethics,* Volume 11, pp. 378-393.

Dunnill, R. & Barham, C., 2007. Confidentiality and security of information. *Anaesthesia and Intensive Care Medicine*, 8(12).

Earle, T. & Siegrist, M., 2008. Trust, Confidence and Cooperation model: a framework for understanding the relation between trust and risk perception. *International Journal of Global Environmental Issues,* 8(1/2), pp. 17-29.

Falcone, R. & Castelfranchi, C., 2001. Social trust: a cognitive approach. In: *Trust and deception in virtual societies.* Norwell, MA: Kluwer Academic Publishers, pp. 55-90.

Flowerday, S. & von Solms, R., 2006. *Trust: an Element of Information Security.* Karlstad, Springer.

Flowerday, S. & von Solms, R., 2007. What constitutes information integrity?. *South African Journal of Information Management, 9(4).*

Gerntholtz, T., van Heerden, M. V. & Vine, D. G., 2007. Electronic medical records - why should you consider implementing an EMR?. *CME,* 25(1), pp. 24-28.

Goodman, K. W., 2008. Health Information Technology: Challenges in Ethics, Science, and Uncertainty. In: K. E. Himma & H. T. Tavani, eds. *The Handbook of Information and Computer Ethics.* Hoboken, New Jersey: John Wiley & Sons, pp. 293-309.

Gostin, L., 1997. Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations. *Annals of Internal Medicine,* 15 October, 127(8 (Part 2)), pp. 683-690.

Gostin, L., 2001. Health Information: Reconciling Personal Privacy with the Public Good of Human Health. *Health Care Analysis,* Volume 9, pp. 321-335.

Grams, R. R. & Moyer, E. H., 1997. The Search for the Elusive Electronic Medical Record System - Medical Liability, the Missing Factor. *Journal of Medical Systems,* 21(1), pp. 1-10.

Grandison, T. & Bhatti, R., 2010. *HIPAA Compliance and Patient Privacy Protection.* Cape Town, IOS Press, pp. 884-888.

Gregor, S., 2006. The Nature of Theory in Information Systems. *MIS Quarterly,* 30(3), pp. 611-642.

Guba, E. G. & Lincoln, Y. S., 1994. Competing Paradigms in Qualitative Research. In: *Handbook of Qualitative Research.* Thousand Oaks: Sage, pp. 105-117.

Heeks, R., 2006. Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics,* Volume 75, pp. 125-137.

Herold, R., 2011. *Managing an Information Security and Privacy Awareness and Training Program.* 2 ed. London: CRC Press.

Hevner, A., 2012. *Knowledge Contributions in Design Science Research.* Irene: SAICSIT 2012.

Hevner, A. R., March, S. T., Park, J. & Ram, S., 2004. Design Science in Information Systems Research. *MIS Quarterly,* 28(1), pp. 75-105.

HPCSA, 2007. *Confidentiality: Protecting and Providing Information.* [Online] Available at: http://www.hpcsa.co.za/downloads/conduct_ethics/rules/confidentiality_protecting_providing_info.pdf [Accessed 17 December 2012].

Huang, J. & Fox, M. S., 2006. *An Ontology of Trust - Formal Semantics and Transivity.* Fredericton, Canada, ICEC.

Introna, L. D., 1997. Privacy and the Computer: Why we need privacy in the Information Society. *Metaphilosophy,* July, 28(3), pp. 259-275.

Introna, L. D. & Pouloudi, A., 1999. Privacy in the Information Age: Stakeholders, Interests and Values. *Journal of Business Ethics,* Volume 22, pp. 27-38.

ISO/IEC 27799, 2008. *Health informatics - Information security management in health using ISO/IEC 27002,* Geneva: International Standards Organisation.

ISO/IEC 29100, 2011. *Information technology - Security techniques - Privacy framework: Ref. ISO/IEC 29100:2011(E),* Geneva: International Standards Organisation.

ISTPA, 2002. *Privacy Framework V1.1.* [Online] Available at: http://www.istpa.org/pdfs/ISTPAPrivacyFrameworkV1.1.pdf [Accessed 20 September 2010].

ISTPA, 2007. *Analysis of Privacy Principles: Making Privacy Operational.* [Online] Available at: http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf [Accessed 20 September 2010].

Johnson, R. B. & Onwuegbuzie, A. J., 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher,* 33(7), pp. 14-26.

Keyser, T. & Dainty, C., 2005. *The Information Governance Toolkit: Data protection, Caldicott, confidentiality.* Oxford: Radcliffe Publishing.

Klein, H. K. & Myers, M. D., 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Studies. *MIS Quarterly,* March, 23(1), pp. 67-94.

Krauss, S. E., 2005. Research Paradigms and Meaning Making: A Primer. *The Qualitative Report,* December, 10(4), pp. 758-770.

Lacey, D., 2009. *Managing the Human Factors in Information Security.* London: John Wiley & Sons.

Latham, J., 2005. *The Research Prospectus - Getting the "DNA" of your Research Design Right.* [Online] Available at: http://www.johnlatham.info/resources/Prospectus_Paper.pdf [Accessed 2 12 2012].

Lederman, R., 2005. Managing hospital databases: can large hospitals really protect patient data?. *Health Informatics Journal,* 11(3), pp. 201-210.

Li, J., 2010. A Sociotechnical Approach to Evaluating the Impact of ICT on Clinical Care Environments. *The Open Medical Informatics Journal,* Volume 4, pp. 202-205.

Losee, R. M., 1997. A Discipline Independent Definition of Information. *Journal of the American Society for Information Science,* 48(3), pp. 254-269.

Maconachy, C. D., Schou, C. D., Ragsdale, D. & Welch, D., 2001. *A Model for Informative Assurance: An Integrated Approach.* United States Military Academy, West Point, N.Y., Proccedings of the 2001 Workshop on Information Assurance and Security.

March, S. T. & Smith, G. F., 1995. Design and natural science research on information technology.. *Decision Support Systems,* 15(4), pp. 251-266.

Margulis, S. T., 2005. *Privacy and Psychology.* Ottawa, Canada, s.n., pp. 1-26.

Martella, R. C., Nelson, R. & Marchand-Martella, N. E., 1998. *Research Methods - Learning to Become a Critical Research Consumer.* Boston: Allyn and Bacon.

Mayer, R. C., Davis, J. H. & Schoorman, F. D., 1995. An Integrative Model of Organisational Trust. *Academy of Management Review,* 20(3), pp. 709-734.

McCallister, E., Grance, T. & Scarfone, K., 2010. *Guide to Protecting the Confidentiality of Personally Indentifiable Information (PII) - NIST Special Publication 800-122,* Gaithersburg, MA: National Institute of Standards and Technology.

Morgan, D. L., 1996. Focus Groups. *Annual Review of Sociology,* Volume 22, pp. 129-152.

Morgan, G. & Smircich, L., 1980. The Case of Qualitative Research. *The Academy of Management Review,* October, 5(4), pp. 491-500.

Narayanan, A. & Shmatikov, V., 2010. Privacy and Security: Myths and Fallacies of 'Personally Indentifiable Information'. *Communications of the ACM,* June, 53(6), pp. 24-26.

Niehaves, B., 2007. *On Epistemological Diversity in Design Science - New Vistas for A Design-Oriented IS Research?.* Montreal, s.n.

Niehaves, B. & Stahl, B. C., 2006. *Criticality, Epistemology, and Behaviour vs. Design - Information Systems Research across different sets of paradigms.* Goteborg: Universitat Trier.

Nippert-Eng, C., 2010. *Islands of Privacy.* Chicago: University of Chicago Press.

Nissenbaum, H., 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford(California): Stanford University Press.

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

OECD, 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [Online]
Available at:
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines
[Accessed 27 April 2010].

OECD, 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* [Online]
Available at: http://www.oecd.org/dataoecd/16/22/15582260.pdf
[Accessed 27 April 2011].

O'Hara, K., 2004. *Trust: from Socrates to Spin.* Cambridge: Icon Books.

Olivier, M. S., 2004. *Information Technology Research - a practical guide for computer science and informatics.* 2 ed. Pretoria: Van Schaik.

Packer, M. J. & Addison, R. B., 1989. *Entering the circle: Hermeneutic investigation in Psychology.* Albany: State University of New York Press.

Padayachee, K. & Eloff, J. H., 2006. *An Aspect-Oriented Implementation of e-Consent to Foster Trust.* Somerset West, South Africa, Proceedings of SAICSIT.

Petronio, S., 2002. *Boundaries of Privacy: Dialectics of Disclosure.* Albany(New York): SUNY Press.

Petronio, S. & Reierson, J., 2009. Regulating the privacy of confidentiality: Grasping the complexities through Communication Privacy Management Theory. In: *Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications.* New York: Routledge, pp. 365-383.

Ponemon Institute, 2012. *Third Annual Benchmark Study on Patient Privacy & Data Security,* Traverse City, MI: Ponenmon Institute.

Prosser, W. L., 1960. Privacy [a legal analysis]. In: F. D. Schoeman, ed. *Philosophical Dimensions of Privacy: An Anthology (2007).* Cambridge: Cambridge University Press, pp. 104-155.

Rindfleisch, T. C., 1997. Privacy, Information Technology, and Health Care. *Communications of the ACM,* August, 40(8), pp. 93-100.

Rosen, C., 2003. *Liberty, Privacy, and DNA Databases.* [Online]
Available at: http://www.thenewatlantis.com/docLib/TNA01-Rosen.pdf
[Accessed 20 September 2010].

SA Justice Dept, 2009. *Protection of Personal Information Bill of South Africa.* [Online]
Available at: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf
[Accessed 07 10 2010].

SA Medical Research Council, 2005. *Book 1: General Principles including research on children, vulnerable groups, international collaboration and epidemiology.* [Online]
Available at: http://www.sahealthinfo.org/ethics/ethicsbook1.pdf
[Accessed 20 September 2010].

Schoeman, F., 2007. Privacy: philosophical dimensions of the literature. In: F. D. Schoeman, ed. *Philosophical Dimensions of Privacy: an anthology.* Cambridge: Cambridge University Press, pp. 1-33.

Scott, T., Rundall, T. G., Vogt, T. M. & Hsu, J., 2007. *Implementing an Electronic Medical Record System - successes, failures, lessons.* Oxford: Radcliffe Publishing.

Shedroff, N., 1999. Information interaction design: a unified field theory of design. In: R. Jacobson, ed. *Information Design.* Cambridge(MA): MIT Press, pp. 267-292.

Silverman, D., 2011. *Interpreting Qualitative Data - A Guide to the Principles of Qualitative Research.* 4 ed. London: Sage.

Skulmoski, G., Hartman, F. & Krahn, J., 2007. The Delphi Method for Graduate Research. *Journal of Information Technology Education,* Volume 6, pp. 1-21.

Smith, H. J., Dinev, T. & Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quartely,* December, 35(4), pp. 989-1015.

Smith, J., Millberg, S. J. & Burke, S. J., 1996. Information Privacy: Measuring individual's concerns about organisational practices. *MIS Quarterly,* June, 20(2), pp. 167-196.

Solove, D. J., 2008. *Understanding Privacy.* Cambridge(Massachusetts): Harvard University Press.

Sullivan, P., 2012. *Qualitative Data Analysis - using a Dialogical Approach.* London: Sage.

Tavani, H. T., 2008. Informational Privacy: Concepts, Theories, and Controversies. In: K. E. Himma & H. T. Tavani, eds. *The Handbook of Information and Computer Ethics.* Hoboken, New Jersey: John Wiley & Sons, pp. 131-164.

Terry, N. P. & Francis, L. P., 2007. Ensuring the privacy and confidentiality of electronic health records. *U. Ill. Law Review*, p. 681.

Thomson, J. J., 1975. The Right to Privacy. *Philosophy and Public Affairs,* 4(4), pp. 295-314.

Tjora, A. H. & Scambler, G., 2008. Square pegs in round holes: Information systems, hospitals and the significance of contextual awareness. *Social Science & Medicine*, pp. 1-7.

US Health & Human Services Dept, 2003. *Summary of the HIPAA Privacy Rule.* [Online]
Available at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
[Accessed 5 May 2009].

Vaishnavi, V. & Kuechler, W., 2004. *Design Research in Information Systems.* [Online]
Available at: http://www.isworld.org/Researchdesign/drisISworld.htm
[Accessed 01 12 2012].

Veeder, S. B., 2007. *Confidentiality Expectations and Willingness to Disclose Personal Information to a Health-care Provider (PhD Thesis).* Ann Arbor(MI): ProQuest Information & Learning Company.

von Solms, R. & van Niekerk, J., 2011. *Research in Computer Science, Information Systems and Information Technology - Back to the Basics.* Durban: South African Lecturer's Association (SACLA).

Westin, A. F., 1967. *Privacy and Freedom.* New York: Atheneum Publishers.

Whetton, S., 2005. *Health Informatics - A Socio-Technical Perspective.* Oxford: Oxford University Press.

Whiddett, R., Hunter, I., Engelbrecht, T. & Handy, J., 2006. Patients' attitudes towards sharing their health information. *Int. J. of Medical Informatics,* 75(7), pp. 530-541.

Whitley, E. A., 2009. Informational privacy, consent and the "control" of personal data. *Information Security Technical Report,* Volume 14, pp. 154-159.

Whitman, M. E. & Mattord, H. J., 2009. *Principles of Information Security.* 3rd Edition ed. Boston: Course Technology.

Williams, P. A. H., 2008. When trust defies common security sense. *Health Informatics Journal,* Volume 14, pp. 211-221.

Winn, P., 2008. *Katz and the Origin of the "Reasonable Expectation of Privacy" Test.* [Online]
Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1291870
[Accessed 5 September 2010].

Woodward, B., 2001. Confidentiality, Consent and Autonomy in the Physician-Patient Relationship. *Health Care Analysis,* Volume 9, pp. 337-351.

Woodward, B. & Hammerschmidt, D., 2003. Requiring Consent Vs. Waiving Consent for Medical Records Research: A Minnesota Law Vs. the U.S. (HIPAA) Privacy Rule. *Health Care Analysis,* September, 11(3), pp. 207-218.

APPENDIX A: ISSA 2011 – RESEARCH-IN-PROGRESS PAPER

http://icsa.cs.up.ac.za/issa/2011/Proceedings/Research/Baucher_Flowerday.pdf