GUIDELINES FOR SECURE CLOUD-BASED PERSONAL HEALTH RECORDS

Avuya Mxoli

GUIDELINES FOR SECURE CLOUD-BASED PERSONAL HEALTH RECORDS

DISSERTATION

By

Avuya Mxoli

Submitted in fulfilment of the requirements for the degree of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

of the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Prof. Nicky Mostert-Phipps

Co-Supervisor: Prof. Mariana Gerber

March 2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Acknowledgements

My family – A special thanks to my parents, **Mr and Mrs Mxoli** for believing in me. Thank you for reminding me that all is possible with prayer. My friends, thank you for the support and encouragement, when I was feeling the pressure in the final year. To my partner, **Buhle**, thank you for always motivating me – especially in these last few weeks, when I felt as if I was not going to meet my deadline; but you told me to press on and maintain a positive attitude. I value the support you gave me throughout this process.

Supervisor – **Nicky Mostert-Phipps**. You have always seen the potential in me ever since you first became my supervisor. Thank you for always approaching my work with a positive attitude and grace. You always went an extra mile and motivated me along the way – even when I felt like giving up myself. You went over and above your supervisor obligations; and you supported and advised me when I was facing some personal issues. Your support and dedication is much appreciated.

Co-Supervisor – **Mariana Gerber**. Thanks for your input and your willingness to become my co-supervisor. I valued your comments and advice throughout this research process.

Abstract

Traditionally, health records have been stored in paper folders at the physician's consulting rooms – or at the patient's home. Some people stored the health records of their family members, so as to keep a running history of all the medical procedures they went through, and what medications they were given by different physicians at different stages of their lives. Technology has introduced better and safer ways of storing these records, namely, through the use of Personal Health Records (PHRs). With time, different types of PHRs have emerged, i.e. local, remote server-based, and hybrid PHRs. Web-based PHRs fall under the remote server-based PHRs; and recently, a new market in storing PHRs has emerged. Cloud computing has become a trend in storing PHRs in a more accessible and efficient manner. Despite its many benefits, cloud computing has many privacy and security concerns. As a result, the adoption rate of cloud services is not yet very high.

A qualitative and exploratory research design approach was followed in this study, in order to reach the objective of proposing guidelines that could assist PHR providers in selecting a secure Cloud Service Provider (CSP) to store their customers' health data. The research methods that were used include a literature review, systematic literature review, qualitative content analysis, reasoning, argumentation and elite interviews. A systematic literature review and qualitative content analysis were conducted to examine those risks in the cloud environment that could have a negative impact on the secure storing of PHRs. PHRs must satisfy certain dimensions, in order for them to be meaningful for use. While these were highlighted in the research, it also emerged that certain risks affect the PHR dimensions directly, thus threatening the meaningfulness and usability of cloud-based PHRs.

The literature review revealed that specific control measures can be adopted to mitigate the identified risks. These control measures form part of the material used in this study to identify the guidelines for secure cloud-based PHRs.

The guidelines were formulated through the use of reasoning and argumentation. After the guidelines were formulated, elite interviews were conducted, in order to validate and finalize the main research output: i.e. guidelines.

The results of this study may alert PHR providers to the risks that exist in the cloud environment; so that they can make informed decisions when choosing a CSP for storing their customers’ health data.

Chapter 1 – Introduction

Chapter Content

CHAPTER 1: INTRODUCTION

1.1. Background

A Personal Health Record (PHR) is a tool, usually web-based, that allows individuals to capture, share, store and process their medical records in one central place (Kaelber, Jha, Johnston, Middleton, & Bates, 2008; Pagliari, Detmer, & Singleton, 2007; Sunyaev, Kaletsch, Mauro, & Krcmar, 2009). The PHR is typically owned, created and managed by the individual; and it allows him to have a life-long summary of all of his health information in one convenient place. Such a system allows individuals to better manage their health; and it is especially useful for individuals with chronic conditions, such as diabetes and hypertension, or with diseases such as cancer, tuberculosis or HIV/AIDS (Archer, Fevrier-Thomas, Lokker, McKibbon, & Straus, 2011).

Some PHRs allow individuals to set reminders and schedule appointments with healthcare providers. They also provide the functionality to take note of symptoms, track pain and record the side-effects of medication. In certain instances, the PHR also enables individuals to view their laboratory and other test results.

A PHR typically allows an individual to record information on past and current illnesses, allergies, immunisations, medication, procedures, test results and more (Neal, 2008; Tang, Ash, Bates, Overhange, & Sands, 2006). Some PHRs allow caregivers, such as family members or friends access to some of their patient’s medical information. This promotes collaboration between the individual and those taking care of him. Certain PHRs offer a variety of health information, thus giving the patients themselves access to a wide range of reliable health information, data and knowledge that can assist them to improve and eventually better manage their own health (Tang et al., 2006).

Individuals are able to provide their healthcare provider with a detailed summary of their medical history gained from their PHRs. This often accelerates the diagnosis process and ultimately the healing process. Some PHRs allow healthcare providers to make notes to elaborate on the individual's condition. This improves the continuity of care by providing other healthcare providers with a clear description of the individual's health status (NCVHS, 2006). Sharing information with physicians also reduces the chances of having duplicate tests done when consulting with multiple healthcare providers (Kim & Johnson, 2002). PHRs, furthermore, promote the home monitoring of chronic diseases (NCVHS, 2006); and individuals can get advice and encouragement at a convenient time from their physicians and caregivers via a PHR; while they are recovering at home.

They can bring their physicians up-to-date on any changes or new developments in their health with the use of a PHR.

As PHRs are web-based, there are numerous ways in which the data can be stored on the internet; and cloud-computing is one of them (Osterhaus, 2010). Many definitions exist for this term; and it is claimed to be rather difficult to combine them into a widely accepted definition (Geelan, 2009; L. Wang, Laszewski, & Younge, 2010). Cloud computing can succinctly be defined as a broad array of pay-as-you-go applications delivered as a service over the internet, as well as the hardware and software used in the various data centres that provide such services (Geelan, 2009; Sabahi, 2011).

A much more comprehensive definition of cloud computing has been provided by the National Institute of Standards and Technology: "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable Computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2).

Cloud computing has created a great hype in the world of technology; and this may be due to the many advantages that it introduces. Below are some of these advantages (Bégin et al., 2008; Geelan, 2009; Grossman, 2009; Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011; Zhang, Zhang, Chen, & Huo, 2010):

- **Reduced cost:** Because cloud computing is an on-demand service, users pay for capacity, as they need it. This access to services is delivered to users with no upfront capital investment. The cost of entry for smaller firms is dramatically reduced, which makes is easy for third-world countries to afford cloud services as well.

- **Scalability:** The goal of cloud computing is to scale resources up or down dynamically through software Application Programming Interfaces (APIs), depending on the load that the user requires. Cloud-based storage services can manage large amounts of data; hence enlarging the user's computing power.
- **Versatility:** Since cloud computing is not focused on working with certain devices or applications, it is highly flexible and easy to use. It opens new possibilities; as it delivers services that were not possible before, such as mobile interactive applications that are location-aware, environment-aware and context-aware, and that respond in real time to information provided by human users.
- **Ease-of-use:** The cloud's simplicity is drawn from the fact that it uses standard technology that already exists in most operating systems. This means that the complexity is kept on the server-side, making the entry point into the cloud very accessible.
- **Internet-centric:** Cloud computing is moving away from relying solely on a physical computer to store and access the data – towards using a multi-tenant, multi-platform, multi-network and global approach. It provides a virtual data centre for the IT industry to ensure that it can provide services on a very large scale when using the internet.

Because of these advantages and more, PHR providers are leaning increasingly towards using the cloud as their storage facility (Ming, Shucheng, Kui, & Wenjing, 2010). The individual's health record can thus be stored in the cloud, which reduces the operational costs for PHR providers. Table 1.1 clarifies the terms: PHR provider, Cloud Service Provider (CSP), and PHR user; as they will be used throughout this study.

Table 1.1: Definition of terms

Term	Description
PHR provider	The entity providing the PHR system for use by the PHR user (patient).
Cloud Service Provider (CSP)	The entity providing cloud services to the PHR provider.
PHR user	The person (patient) who makes use of a PHR to record his health history. The PHR user is the customer of the PHR provider.

Storing information in the cloud raises discomfort for the users; and as such, people are rather sceptical of using this powerful tool (Armbrust et al., 2010). PHRs stored in the cloud are at a higher risk, because of the security and privacy issues found in the cloud (AbuKhousa, Mohamed, & Al-Jaroodi, 2012). The data stored in a PHR can typically be divided into two categories, namely: Personally Identifiable Information (PII) and Healthcare data. PII consists of information that can be used to identify, locate or contact an individual, e.g. name, address, telephone number, etc. Healthcare data are composed of media files about the individual, such as scans, X-rays, and other types of images and videos (Elmogazy & Bamasak, 2013). This type of information is highly sensitive and should be treated as such.

The security and privacy issues in cloud computing may affect the Cloud Service Providers (CSPs), the developers and the users of cloud applications. The issues that affect users, as provided by the Gartner group (Brodkin, 2008), are discussed below:

- **Privileged user access:** Information on the cloud is not in the control of the user; so it is very difficult to ensure that it is in the right hands. Moreover, CSPs may outsource the storage of their customers' sensitive data. This raises confidentiality issues; since there would then be many parties who have access to the information and to the customer's data. Consequently, the patients' integrity is highly compromised as well.

- **Regulatory compliance:** Inasmuch as the customers' data are held by the CSP, the latter is ultimately responsible for their security and integrity.
- **Data location:** When using the cloud, customers might not necessarily know exactly where the data are located; and this goes as far as not knowing the actual country in which the data are stored!
- **Data segregation:** Data in the cloud are typically in a shared environment with other customers' data (multi-tenancy). Because of this, the data of various customers may reside at the same location, and thus fall prey to intruders.
- **Recovery:** Most cloud services replicate the data and application infrastructure across multiple sites for back-up purposes. Even though customers do not know where the data are located, they should enquire about what happens to the data in the event of a disaster.
- **Investigative support:** Cloud computing makes it difficult to investigate possible inappropriate or illegal activities. This is mainly because of the fact that multiple customers' data may be collocated; and they may also be spread across multiple hosts that are continuously changing.
- **Long-term viability:** Even though it is highly unlikely for CSPs to go broke or to be acquired by a larger company, customers should make sure that their data would remain available. How the data would be returned to the ownership of the customer, and the format in which it would be returned, constitute vital information for which the customer should ask the CSP.

Providers of products and services via cloud computing facilities should therefore be provided with information that would assist them to choose a CSP that is secure and trustworthy.

1.2. Problem description

Storing PHRs in the cloud exposes the users' data to numerous security and privacy risks (AbuKhousa et al., 2012; Subashini & Kavitha, 2011). When PHR providers transfer data to the cloud, they also transfer most of its control.

When the researcher was conducting a literature review for this research, it was discovered that little guidance is given to PHR providers to assist them in making an informed choice, when they select a CSP for the storage of their customers' PHR data. They need to know what to consider when they select a CSP, to ensure that sensitive PHR data would be kept private and secure. Even though countries have data-protection laws that can protect the users' rights, they are not very effective for cloud computing services; because the data in the cloud can be stored anywhere in the world; since the various jurisdictions have different laws (Svantesson & Clarke, 2010).

1.3. Problem statement

There is a lack of guidance to assist PHR providers in making an informed choice when selecting a CSP, to ensure that their customers' data are kept private and secure.

1.4. Research objectives

The primary objective of this research project is to propose guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data remain private and secure. The primary objective is supported by the following secondary objectives:

- Define Personal Health Records and cloud computing.
- Identify information security risks of which the PHR providers should be aware when storing their customers' data in the cloud.
- Identify the various control measures, based on recognized best practices and frameworks, which can be used to mitigate the identified risks.
- Formulate guidelines that would assist PHR providers in choosing a secure CSP.

1.5. Delineation

This research will focus on the information security risks that may affect PHRs that are stored in the cloud. After these risks have been identified, security measures to mitigate them will be presented; and these will be in the form of guidelines. These guidelines are aimed at any PHR providers: whether they offer PHR services to customers in the public or private healthcare sectors.

The way that data are stored in cloud-computing makes it difficult to know in which country they are located, thus making it difficult to apply certain data-protection laws; as these differ, according to local jurisdiction. In the light of such matters, this study is not aimed at any particular country.

1.6. Research methodology

The above section provided the problem statement and the research objectives that aim at addressing the problem. This section will describe the methods that have been implemented to accomplish the research objectives, which will ultimately address the problem statement. Research methodology includes the procedures that researchers use, in order to describe, explain and predict the phenomena involved in their work (Rajasekar, Philominathan, & Chinnathambi, 2006).

The following subsections will describe the research methodology associated with this research study.

1.6.1. The research strategy

When conducting research, researchers have the option of adopting one or both of the following research strategies (Creswell, 2013):

- Quantitative: This research strategy is based on measuring quantities or the amount involved in the collection and analysis of the data (Bryman, 2012; Rajasekar et al., 2006).

- Qualitative: This research strategy employs a naturalistic approach that aims at understanding the phenomena in context-specific settings (Golafshani, 2003).

Thompson states that if the aim of the research is exploratory; and it seeks to bring about an understanding on an area where little is known; then qualitative methodologies would be appropriate (2011). This research study is exploratory in nature; as it aims to evaluate existing studies, in order to identify the known information security risks that PHR providers should be aware of when storing their customers' data in the cloud. In addition, control measures based on recognized best practices and frameworks will be identified, which can be used to mitigate such risks. Based on the identified risks and control measures, guidelines will be formulated to assist PHR providers in making an informed choice, when selecting a CSP to ensure that their customers' data remain private and secure. As such, a qualitative research strategy has been adopted for this research; and qualitative methods have been employed, in order to formulate the guidelines for secure cloud-based PHRs.

The following subsection describes the methods that were used to address the research problem, as stated; how they were used; and why they should lead to a solution to the research problem.

1.6.2. Research methods

Table 1.2 indicates the research methods that were employed to achieve the research objectives.

Table 1.2: Research objectives and research methods

Research objective	Research method
Define Personal Health Records and cloud computing.	Literature review
Identify security and privacy risks that PHR providers should be aware of when storing their customers' data in the cloud.	Systematic literature review Qualitative content analysis
Identify control measures, based on recognized best practices and frameworks, which can be used to mitigate the identified risks.	Literature review Argumentation
Formulate guidelines that will assist PHR providers in choosing a secure CSP.	Reasoning Argumentation Elite interview

Below are explanations/definitions for the research methods that were used:

- **Literature review:** An iterative process, where a researcher finds some material, works on it, decides what to keep and what to discard, and then uses what has been learnt to search for more information (Olivier, 2009). For this study, a number of literature sources – ranging from journal papers, conference papers, website articles, book chapters, etc., were consulted, in order to conduct an in-depth study and to gain a comprehensive background on the previous knowledge on related topics. These sources are what the researcher used, in order to identify the information security risks, as well as the control measures that can be used to mitigate these risks.

- **Systematic literature review:** Fink (2005) describes this as “a systematic, explicit, comprehensive, and reproducible method for identifying, evaluating, and interpreting the existing body of original work produced by researchers, scholars, and practitioners.” (Fink, 2005, p. 36). This method was used in order to identify literature that will assist in identifying information security risks that PHR providers should be aware of when storing their customers’ data in the cloud.
- **Qualitative content analysis:** Content analysis is a research method used to systematically analyse informational contents found in textual data (Forman & Damschroder, 2007). It can either be qualitative or quantitative. For this research study, the qualitative approach was adopted. Qualitative content analysis examines data that is acquired through an open-ended data collection process where the purpose is to get the detail and depth of the information instead of measurement (Forman & Damschroder, 2007). After the systematic literature review, this technique was used to further analyse the literature that was selected for inclusion in the study.
- **Reasoning: “**The process of thinking about something in a logical way, in order to form a conclusion or judgment”, as defined in (Reasoning, n.d.). This method was used in the formulation of the guidelines, in order to ensure that appropriate guidelines are developed in this study; and this was based on how the identified control measures, as indicated by the relevant ISO controls, best address the identified information security risks.
- **Argumentation:** A combination of known facts used to derive new facts. It may be used to refer to an entire reasoning about a certain aspect in a system, or to refer to one building block in the reasoning (Olivier, 2009). Argumentation was used in formulating the guidelines, as the output of this research; but it was also used throughout the study in identifying and using material relevant for use, in order to adequately address the research objectives.

- **Elite interview:** Elite individuals are described as people who are considered superior, influential and/or well-informed, in terms of ability or qualities compared to the rest of an organization or community (“Elite,” 2016; Marshall & Rossman, 2011). Elite interviews are used, in order to validate what has been established from other sources, to ascertain what a set of people think, to interpret decisions gathered from a larger population, or to reconstruct an event or set of events (Tansey, 2007). With the development in technology, i.e. the use of the Internet and Electronic mail (E-mail), it has been discovered that there are more improved ways to gain access to the elites (Harvey, 2010). Elite interviews will be used in this research in order to validate the guidelines that will be produced as an output of this study and they will be conducted via E-mail. The elite interviews will assist in demonstrating research rigour, as well as to gather the viewpoints of the elites on the guidelines, which would assist in producing useful guidelines. More on the elite interviews will be discussed in the evaluation chapter, Chapter 05.

1.6.3. The research process

A general literature review was conducted to define Personal Health Records and cloud computing. This helped the researcher to formulate a background chapter that would create a basis for the study.

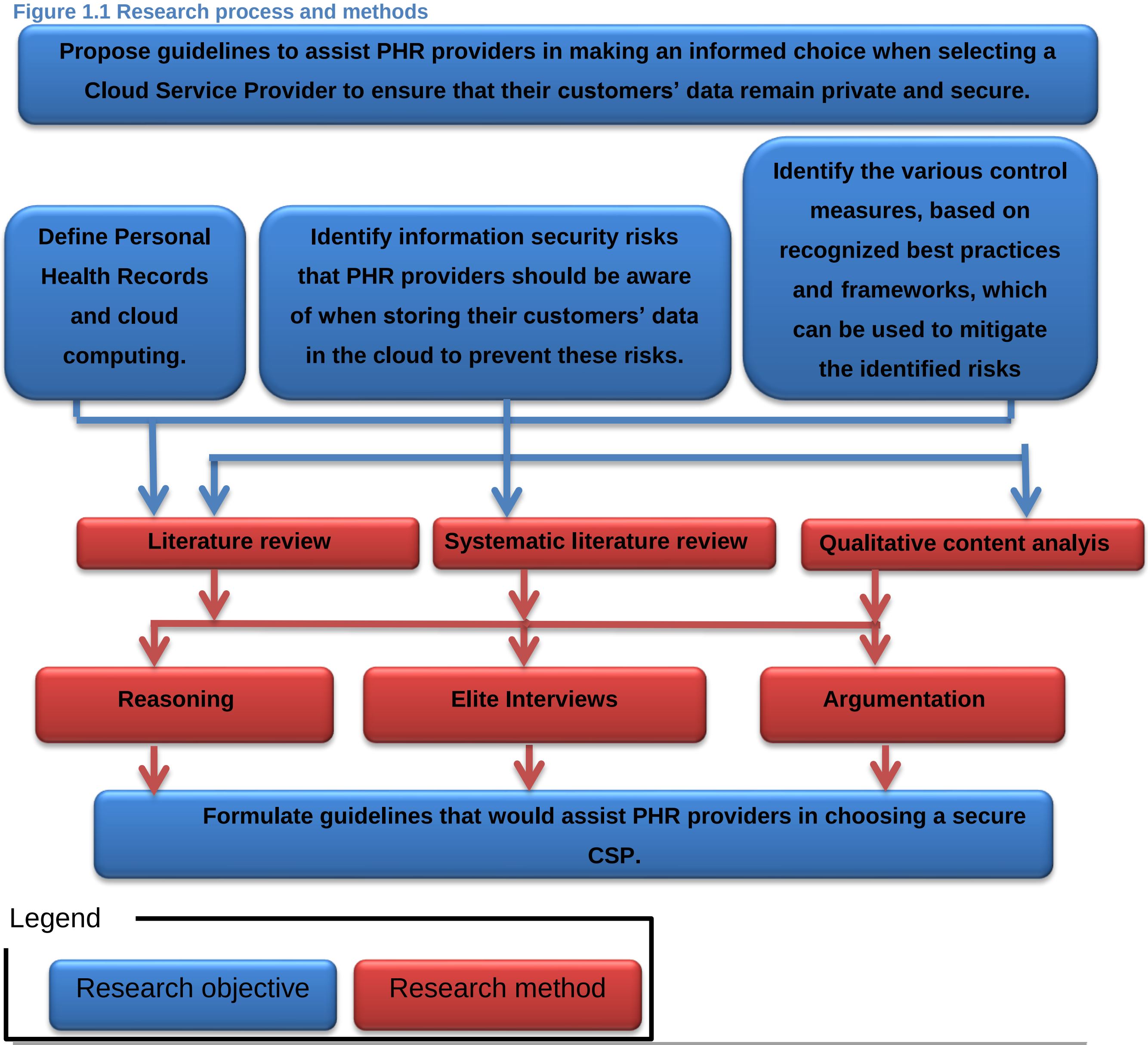
A detailed literature review was conducted and it revealed that for a PHR to be deemed useful, it should have certain dimensions, which are mentioned in Chapter 2. A systematic literature review was further conducted to identify security and privacy risks of which PHR providers should be aware when storing data in the cloud, and it was discovered that PHR dimensions may be negatively impacted by these risks. An elite interview was conducted, in order to validate the classification of the information security risks that may impact the PHR dimensions.

Another detailed literature review was subsequently conducted, in order to identify control measures that could be used to mitigate the identified risks. This assisted the researcher to develop appropriate guidelines.

Guidelines for secure cloud-based PHRs were formulated, based on the identified security and privacy risks, as well as the measures that could be taken to manage these risks, as identified via the literature review. The formulation of these guidelines employed argumentation and reasoning, based on the results of the literature review. Elite interviews were also conducted, in order to further refine and validate the guidelines.

Finally, the research was concluded and compiled into a dissertation document.
A summary of the research process is presented in Figure 1.1.

Figure 1.1 Research process and methods



1.7. Chapter outline

- **Chapter One** introduces the research by focusing on the problem statement, the research objectives, the research methods that were used, as well as the research process that was followed to complete the research.
- **Chapter Two** provides an overview of Personal Health Records (PHRs) and cloud computing.
- **Chapter Three** reports on the security and privacy risks that have been identified and of which users should be aware, when storing their data in the cloud.
- **Chapter Four** describes how the guidelines are formulated to assist PHR providers in making an informed choice, when selecting a Cloud Service Provider. The guidelines themselves are also presented in this chapter.
- **Chapter Five** presents the validation approach that was used for this study.
- **Chapter Six** concludes the research by providing a summary of what was discussed and mentioning how the study should benefit the general public.
- **Appendix A** presents a published paper that was a work-in progress, and which contributed to the identification of information security risks (see Table 4.1 Page 45) as well as the development of the guidelines (see Table 4.2, Page 55).
- **Appendix B** presents published papers that were written during the background literature review stage of this research. Whilst these papers do not directly contribute to this research project, they did assist the researcher in defining and describing PHRs.
- **Appendix C1** is a background document for the Part 1 section of the elite interviews.
- **Appendix C2** is a questionnaire for the Part 1 section of the elite interviews.
- **Appendix C3** is a completed questionnaire for the Part 1 section of the elite interviews.
- **Appendix D1** is a background document for the Part 2 section of the elite interviews.
- **Appendix D2** is a questionnaire for the Part 2 section of the elite interviews.
- **Appendix D3** contains completed questionnaires for the Part 2 section of the elite interviews.

- **Appendix E** is a language certificate from the proof reader.

1.8. Conclusion

This chapter serves as the introduction to the research at hand. It gives the reader an indication of what the dissertation will contain, as well as the structure and layout that has been followed. The problem statement is presented here, in addition to the research objectives. The research methodology is defined; and the scope of the research has been specified. The following chapter will present the literature review on PHRs and cloud computing.

Chapter 2 – Personal Health Records and cloud computing

Chapter Content

CHAPTER 2: PERSONAL HEALTH RECORDS AND CLOUD COMPUTING

2.1. Introduction

This chapter describes the concept of Personal Health Records (PHRs) and cloud computing in more detail, expanding on what was briefly introduced in Chapter 01. The concept of cloud-based PHRs is also introduced briefly, in order to link these two sections together.

2.2. Personal Health Records

This section describes Personal Health Records (PHRs) i.e. definitions, benefits and barriers to adoption.

Traditionally, the personal health information of patients was kept in paper folders in the physician's consulting rooms (Detmer, Bloomrosen, Raymond, & Tang, 2008). Every time a patient visited a new physician, he had to fill in his personal information, in order to create a file. This information remained at that particular practice; and hence, there was a need to create a new file every time the patient consulted a new physician. Patients were allowed to request copies of their health records from their physicians, in order to keep a personal history of their health information at home, or to take to a new physician (Maloney & Wright, 2010).

It is especially important for patients with chronic conditions to keep track of their health information and health history (Fuji et al., 2012). These paper-based health records can be difficult to manage, and are prone to being damaged and/or lost.

Nowadays, a far more convenient web-based tool can be used in the form of a Personal Health Record (PHR). A PHR can be defined as a web-based application that an individual may use to record, store, access, share and manage his own health information in one place (Endsley, Kibbe, Linares, & Colorafi, 2006). Since a PHR is owned by the individual, he can decide with whom to share it, e.g. physicians, caregivers or family members. When sharing it, the patient also has the freedom to choose, which parts to make available, and which ones to keep personal.

The following subsection will give some requirements that need to be satisfied for a PHR to be considered useful.

2.2.1 PHR Dimensions

In order for a PHR to be deemed useful, it has to satisfy the requirements associated with nine (9) dimensions, as identified by van der Westhuizen (2012). These dimensions and the associated requirements are listed and described briefly in Table 2.1.

Table 2.1: PHR dimensions

DIMENSION	REQUIREMENT
CONFIDENTIALITY	PHRs must only be accessible to authorised parties.
INTEGRITY	No unauthorised additions, deletions or alterations. Edits must be tracked by auditing logs.
AVAILABILITY	PHRs must be accessible to both the individual and the physician (if access is granted) all the time. Emergency access must also be enabled.
AUDITABILITY	PHRs should contain audit logs to track access, changes, additions and deletions. They must also support non-repudiation.
ACCURACY	Information must be captured accurately and correctly by implementing tools that prevent human error.

Continuation of Table 2.1

DIMENSION	REQUIREMENT
COMPLETENESS	PHRs must not only contain basic personal information, physician visits, check-up notes and diagnoses, but also information, such as diet and exercise logs, health insurance information, etc. in order for them to be considered complete.
APOMEDIATION	PHRs should educate individuals and assist them in capturing the record with a sense of understanding. Individuals must also have the ability to interact with one another and with the physicians.
PRIVACY	An individual must have the ability to grant or refuse (including legally) access to his PHR.
INTEROPERABILITY	Ability to interoperate with other health systems, so as to interchange health information. Importing and exporting of data into health standards must also be enabled in a PHR.

The subsection below discusses some PHR types.

2.2.2. Types of PHRs

Personal Health Records come in different forms, depending on their storage location. They can be local, remote server-based, or hybrid (Steele, Min, & Lo, 2012); and these different types will be discussed below (Detmer et al., 2008; Koufi, Malamateniou, & Vassilacopoulos, 2010; Robison, Bai, Mastrogiannis, Tan, & Wu, 2012; Steele et al., 2012).

- **Local PHRs**: Stored locally on a portable storage device, and do not need a network connection. Examples of such PHRs include:

    - Paper-based PHRs: The folders that individuals keep for themselves collected from different physicians.
    - Device-based PHRs: Records stored on a portable device, such as a USB, or in a personal computer.
- **Remote server-based PHRs:** Stored via the internet, for example:
    - Web-based PHRs: Stored on the internet, and can be accessed anywhere and anytime, so long as there is an active internet connection. These typically use a web-based online server that is managed by a healthcare provider.
    - Cloud-based PHRs: Web-based PHRs stored in a cloud computing environment. They use virtual and dispersed servers and storage under interconnected networks.
- **Hybrid PHRs:** Allow an individual to duplicate his data in both a local and remote location. This promotes availability and flexible access.

This subsection discussed different types of PHRs. For the remainder of this dissertation, the term PHR will refer to a cloud-based PHR; since this is the focus of this research project.

2.2.3. Benefits associated with PHRs

This subsection briefly discusses some of the benefits of using a PHR. The benefits will be divided, according to the following categories: Patient-related; caregiver and physician-related; and economy-related (Tang et al., 2006; Kaelber et al., 2008; Steele et al., 2012; Sands, 2007; Witry, Doucette, Daly, Levy, & Chrischilles, 2010; Keckley & Chung, 2010).

- **Patient-related**:
    - Increased patient safety: patients can use the PHR to look for drug interactions and contra-indications.
    - Enhanced efficiency: patients can gain access to their health information with minimal effort and expenditure.

  - Better patient satisfaction, in terms of how well they can manage their health information, in cases of both acute and chronic conditions.
  - Reasonable ease-of-use: PHRs support multiple-user views; and they allow for user-friendly interactions, such as the input and output of data.
  - Greater patient access to a wide array of credible health information.
  - Disease-tracking: patients can use the PHR to track their diseases to see their progress, and also get early intervention when they come across a problem.
  - More engagement in their health process, which would yield better health outcomes.
- **Caregiver and physician-related**:
  - Lower communication barriers between patient and physicians; since they are no longer limited to face-to-face interactions.
  - Improved quality of care: the physician would have a better health history of the patient, thus having a clearer picture of the patient's condition.
  - Ongoing connection between the patient and the physician.
  - Assists physicians when making decisions; because they have a record of what tests, diagnoses, medications, and treatments have already been administered to the patient. This also decreases the chances of repeating and wasting resources.
  - Improved sharing of medical records amongst physicians, specialists, laboratories and other healthcare facilities that a patient may have visited.
  - A patient's health record becomes readily available in an emergency situation, which improves the chances of being properly treated.
  - A patient who has his own health record ensures that there is a copy of the record – in case the one at the physician's office gets lost or damaged.
- **Economy-related**:
  - PHRs offer healthcare organisations overall reduced healthcare costs; since they help avoid duplicate tests; because test results are easily available across different facilities. There will be fewer admissions and visits to the emergency

room, which reduces costs for the medical aid companies. PHRs that help patients with managing their chronic diseases also yield lower chronic disease-management costs.

Although PHRs come with these benefits and more, there are still adoption barriers to consider; and these will be discussed in the following subsection.

2.2.4. Barriers to the adoption of PHRs

This subsection will mention some of the adoption barriers to PHRs (Steele et al,, 2012; Lober et al., 2006; Witry et al., 2010; Tang et al., 2006; Carrion, Fernandez Aleman, & Toval, 2012):

- **Digital divide** – There is the problem of access to computers, which may limit a certain population from gaining access to their PHRs.
- **Privacy and security concerns** – Patients are always wary about accessing sensitive information on the internet. PHR users worry that once their health information is made available on the internet, they would be vulnerable to being hacked.
- **Legal concerns** – Physicians worry that PHR use might have legal implications for them. For instance, if a physician relies on data that have been inaccurately entered by a patient to make a diagnosis, he may be charged for negligence in a court of law.
- **User interface and usability issues** – Patients with disabilities (cognitive or physical) may recognise the need to use a PHR; but they may not be able to do that without assistance, because the interface may not necessarily cater for them. The same goes for the elderly, who may want to use a PHR; but due to the latter's design, they may end up not being able to use it.
- **Inaccuracy of data entered by patients** – Physicians worry that patients may enter inaccurate information on their PHRs, because of their lack of a health background. This would cause them not to trust the PHR data; and this might render such data useless at the end of the day.

- **Medical terms** – Patients may not understand the medical terms that their physicians enter into their PHRs; and this may cause unnecessary panic. Physicians may be induced to limit what they write on the PHR – for fear of causing alarm.

This section gave an overview of PHRs – definitions, benefits and adoption barriers. Despite the barriers mentioned above, PHRs can still play a significant role in improving the health of individuals. They can be stored on the internet by making use of cloud computing storage services. Cloud computing is the use of applications and hardware systems delivered over the internet as a service (Armbrust et al., 2010). PHRs that are accessed via cloud computing are known as cloud-based PHRs (see subsection 2.2.1). These will be discussed in more detail in the following section.

2.3. Cloud-based PHRs

This section provides a brief background on cloud-based PHRs, which provide more flexibility and agility to the procedures for accessing, processing and storing patient data. Cloud-based PHRs can be implemented in one of two ways (Steele et al., 2012):

- Isolated healthcare providers interconnected under one CSP, or
- individuals' virtual PHRs implemented in a cloud computing environment that is separate from that of the healthcare provider.

Cloud-based PHRs offer a solution to the problem of having dispersed patient data across multiple institutions. When stored in the cloud, PHRs could be stored in a virtual generic archive and accessed by healthcare providers when permission is granted by the PHR owner. This promotes the sharing of the patient's health record (Koufi et al., 2010).

The next section will focus on the concept of cloud computing.

2.4. Cloud computing

A broader description of cloud computing follows below and details on its benefits, features, service and deployment models are also provided.

Cloud computing comes in two forms: it provides additional computing instances; and it is also designed to support data-intensive applications through its scaling capacity (Grossman, 2009). It can be provided via computing power, storage or platforms that are distributed on demand to external customers, thus promoting an economy-of-scale (Armbrust et al., 2010; Foster, Zhao, Raicu, & Lu, 2008).

Some of the features of cloud computing include the following (Mell & Grance, 2011; SATW, 2011; Armbrust et al., 2010):

- **Rapid elasticity** – Cloud computing resources can be scaled up or down, as needed. Organisations can better meet and support business needs and react more rapidly to customers' demands.
- **Measured service** – Cloud computing can be encapsulated as an abstract entity that delivers different levels of services to a variety of customers.
- **On-demand self-service** – Services can be dynamically configured and delivered on demand – without any manual intervention.
- **Broad network access** – Cloud computing services can be accessed via a wide array of devices, such as mobile phones, tablets, laptops, etc.
- **Resource pooling** – The CSP's resources are pooled, in order to serve many different customers through multi-tenancy. They share virtual and physical resources, which are assigned and re-assigned, according to customer demand.

Cloud computing features/characteristics are to be described in this subsection. Next, there follows a discussion of the various service models of cloud computing.

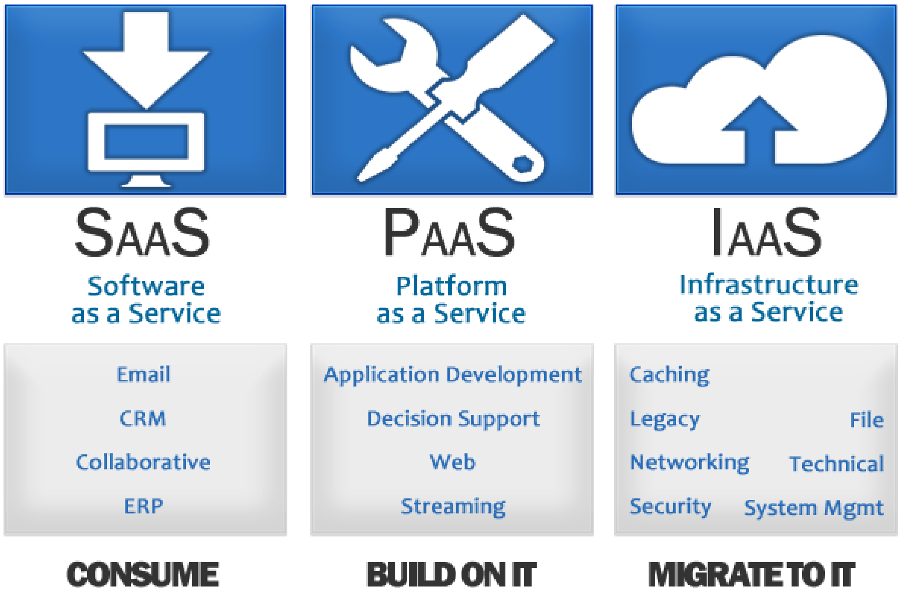
2.4.1. Service models

The services provided by cloud computing are categorised under three models, as described below (Gong, Liu, Zhang, Chen, & Gong, 2010; Mell & Grance, 2011; Wang, et al., 2010; Baliga, Ayre, Hinton, & Tucker, 2011; Grossman, 2009):

- **Software as a Service (SaaS) –** Customers who use this model of cloud computing are provided with software or applications over the internet without having to install the applications on their local computers. They follow the pay-per-use pattern, which greatly reduces their costs; and they no longer have the burden of software maintenance. **Infrastructure as a Service (IaaS) –** Through this service, customers can outsource their storage, processing, networks and other important resources to the cloud. However, they do not manage or control the underlying infrastructure.
- **Platform as a Service (PaaS) –** This is the middle layer between hardware and software/application. PaaS allows the customer to deploy applications to the cloud infrastructure, thus giving over-the-network server, operating systems or storage management and control to the CSP.

Figure 2.1 gives a visual representation of these service models, together with examples of how they are used. For example, SaaS can be employed to offer Emails, Customer Relations Management (CRM) software, Collaboration tools and Enterprise Resource Planning (ERP) software. IaaS can be used to offer caching, legacy file networking, technical security system management; and PaaS can be used for application development, decision-support and web-streaming.

Figure 2.1:Service models (Nguyen, 2015)



This subsection highlighted the different services, in which cloud computing resources can be used. The next subsection gives a brief description of the different deployment models of cloud computing.

2.4.2. Deployment models

Cloud computing can be provided in the following deployment models (Zhang & Liu, 2010; Mell & Grance, 2011; SATW, 2012):

- **Private cloud** – This type of cloud is used by an organisation, which can decide to run it themselves, or to have a CSP run it externally.
- **Community cloud** – A group of organisations that share the same goal/mission can use this type of cloud infrastructure. It may be managed by the group; or they may have an external party to manage it.
- **Public cloud** – This is made available to the general public, and is owned by a CSP.
- **Hybrid cloud** – This involves a combination of two or more clouds (e.g. private, community or public). It combines the benefits gained from all the different kinds of deployment models, e.g. an organisation may choose to have its public

data/applications run via a public cloud; while all the sensitive organisational information will be run via a private cloud.

This subsection has highlighted the various cloud computing deployment models. The following subsections highlight the benefits and drawbacks of cloud computing.

2.4.3. Benefits of cloud computing

This subsection briefly describes some of the benefits of cloud computing (Armbrust et al., 2010; Hwang & Li, 2010; SATW, 2012; Grossman, 2009):

- **Cost containment** – Organisations that use cloud computing can save money; because they would no longer have to provide their own IT infrastructure, or carry maintenance and training costs. Organisations do not even need to incur start-up capital expenses, because of the pay-per-use characteristic of cloud computing.
- **Innovation speed** – Cloud services can be provided more quickly, which allows a business to respond rapidly to changes and to meet customer demands in a timely manner.
- **Availability** – CSPs can deliver resources at a high-availability rate, due to their ability to scale and the redundant interconnection and load-balancing abilities.
- **Efficiency** – Cloud computing provides efficient IT resources to an organisation; so that it is free to focus on other business functions. This promotes high growth and sustainability in the business.
- **Improved information hiding** – Users of cloud services can have unnecessary information hidden, thus making it easier to control their core business parameters.

Although cloud computing offers such great benefits and more, there are unfortunately also some disadvantages to it. The next subsection briefly discusses some of the drawbacks of cloud computing.

2.4.4. Drawbacks of cloud computing

This subsection highlights some of the implications that come with the use of cloud computing.

- **Performance unpredictability** – Network and disk input/output is problematic in cloud computing. It introduces a strong dependence on the availability of networks and infrastructure; and as a result, the cloud cannot be accessed without them (Armbrust et al., 2010).
- **Customisability issues** – Applications in the cloud do not necessarily allow you to customise the data as you might want. This makes it difficult to have unique applications and services (Akande, April, Van Belle, Town, & Belle, 2013).
- **Long-term costs** – The data-centre subscription fee may in the long run potentially cost more than would buying the hardware (Pocatilu, Alecu, & Vetrici, 2010).
- **Reputation fate sharing** – Cloud computing allows for the sharing of hardware resources; and this introduces problems if one user's application compromises the system (Grossman, 2009). When one of the users in the same cloud environment displays bad behaviour; it could affect the reputation of the others using the same cloud (Armbrust et al., 2010).
- **Security** – The data stored in the cloud are prone to unauthorised access from the CSP's staff members, and any other third parties involved. This introduces a wide spectrum of security and privacy risks (Armbrust et al., 2010).

Some of the prominent cloud computing drawbacks have been discussed in this subsection; the security and privacy issues will be discussed in more detail in Chapter 3.

2.5. Conclusion

This chapter has described Personal Health Records (PHRs) in detail, focusing on the definition, types, benefits and barriers to adoption. Cloud computing was introduced as a way that PHRs can be stored and accessed over the internet i.e. through the use of cloud-based PHRs. Cloud computing was further explained in terms of its features, service models, deployment models, benefits and drawbacks. This has provided a background on the focus of the study at hand, i.e. cloud-based PHRs. This chapter's output helped to meet the sub-objective: "Define Personal Health Records and cloud computing" The next chapter will deal with the risks that come with storing PHRs in the cloud.

Chapter 3 – Information security risks relating to cloud-based Personal Health Records

Chapter Content

CHAPTER 3: INFORMATION SECURITY RISKS RELATING TO CLOUD-BASED PERSONAL HEALTH RECORDS

3.1. Introduction

The previous chapter provided a detailed background on Personal Health Records and cloud computing. It introduced the two topics and how they link together for the purpose of this research. In this chapter the process that was followed in order to obtain literature for its content will be described. Information security risks relating to cloud computing, focusing specifically on cloud-based PHRs will also be introduced here. The concept of information security will also be discussed, in order to provide some background on why information needs to be protected. This will lead to a discussion of the risks that are related to the use of the internet in general; this will be followed by cloud computing-specific risks. These risks will be categorised in terms of their information security aspects. The information security risks will be linked to PHRs in terms of how they can affect the personal information stored in the cloud.

3.2. Research process followed to obtain literature

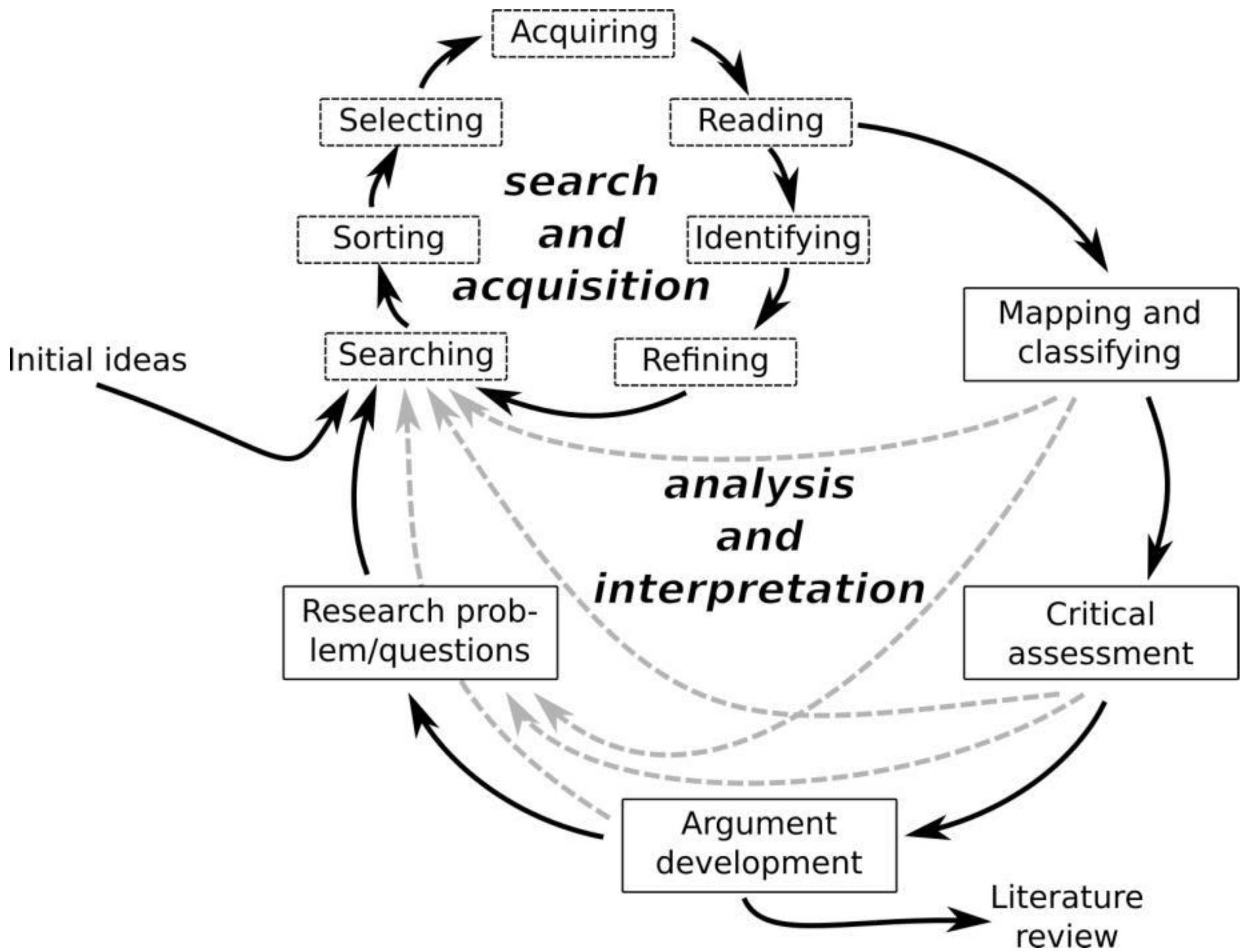
As mentioned in Chapter 1, two research methods were used in order to identify the risks presented in this chapter. Okoli and Schabram (2010) state that in order to portray rigour in a literature review, a systematic literature review must follow a methodological approach. Firstly, it must be explicit in explaining how it was conducted. Secondly it must comprehensively describe the criteria that used to define the scope of literature to be included. Finally, it must be able to be reproduced by other researchers who would adopt the same review approach (Okoli & Schabram, 2010). This approach was deemed fitting for this research study as the results need to be validated in order to strengthen how the study was conducted.

The hermeneutic framework for the literature review process described in Boell and Cecez-Kecmanovic (2014) gives the process that takes place when one conducts a literature review, as seen in Figure 3.1 below. The smaller circle shows the initial process of going through the material in order to identify and acquire those articles that will be used for the study. This process can be mapped with the stages described by Okoli and Schabram (2010) which describe how to go about conducting a systematic literature review. Only the smaller circle was included as part of the research approach adopted by the researcher.

Guidelines on qualitative content analysis by Elo and Kyngas (2007) were adopted in the last stage of the systematic literature review. Elo and Kyngas (2007) further base qualitative content analysis on three steps:

- Preparation: In this step the researcher begins by selecting a unit of analysis. This can range from a word, phrase, or theme. The researcher then makes sense of the data in order to learn what the articles are talking about.
- Organization: The data obtained from the step above is then categorized. This can be done through open coding, categorization and abstraction.
- Reporting: The researcher then reports on the process of analysis as well as on the results of the study.

Figure 3.1 A hermeneutic approach framework for the literature review process consisting of two major hermeneutic circles (Boell & Cecez-Kecmanovic, 2014)



The following stages were identified from Okoli and Schabra (2010):

- Stage 1: Planning – The purpose of the literature review and the protocol to be followed are identified in this stage (Okoli & Schabram, 2010). For this research study, the purpose of the literature review was to identify information security risks that PHR providers should be aware of when storing their customers' data in the cloud. When conducting this systematic search, Webster and Watson (2009) state that the researcher should ensure that a relatively comprehensive census of relevant literature is accumulated. After this is done, a protocol needs to be defined. A protocol describes the procedure that will be followed in conducting the review (Okoli & Schabram, 2010). For this study the protocol specifies the databases to be searched, the search phrases or keywords to be used, the time-frame of articles and type of articles to be searched to achieve the purpose of the literature review. Searching for literature may assist the researcher in identifying literature that will add quality to the study (Boell & Cecez-Kecmanovic, 2014).

- Stage 2: Selection – This involves the description of how the search was conducted and also the practical screening i.e. stating the criteria used for the inclusion and exclusion of literature (Okoli & Schabram, 2010). Sorting also takes place in this stage as the researcher selects those articles that are relevant to the study (Boell & Cecez-Kecmanovic, 2014). The Google Scholar search engine was primarily used in the initial search. Additional databases searched included Research Gate, CSIR Information Services, IEEE and Science Direct. The keywords and phrases used were information security, risks, personal health records, phr, cloud computing, privacy, and threats. The time-frame was from 2006-2014. The types of articles included full-text journal articles, conference proceedings and books. The search was conducted between November 2014 and July 2015. The articles that were retrieved from the abovementioned search were screened in order to determine their relevance for inclusion. The most crucial criterion that the articles had to fulfil was that of complying with the objective that this research method seeks to satisfy i.e. to identify information security risks that PHR providers should be aware of when storing their customers' data in the cloud. Furthermore, the article had to be in English, published between 2006 and 2014, and in full text.
- Stage 3: Extraction – Quality appraisal and data extraction are performed in this stage in order to screen articles for exclusion and after that has been done, extract the relevant information from those chosen for inclusion (Boell & Cecez-Kecmanovic, 2014; Okoli & Schabram, 2010). Reading, identifying and refining were also done in this stage. Reading may lead to the further selection of more material which will be further analysed for inclusion (Boell & Cecez-Kecmanovic,

- 2014). The publication title and abstract were used to screen the articles for relevance. This, according to Boell and Cecez-Kecmanovic (2014) is the refining of literature to improve the search. Mendeley was used as the referencing tool for this study and the feature of removing duplicates was used to further sift through the articles. More publications were identified through citation tracking from the articles that were already identified (Boell & Cecez-Kecmanovic, 2014). This led to a total of 57 articles that were selected for further review, from which a total of 46 articles was further reviewed for quality appraisal, which entailed that the articles had to be peer-reviewed.
- Stage 4: Execution – This stage is comprised of the synthesis of the study as well as writing the review (Okoli & Schabram, 2010). An analysis has to be followed in order to combine the information from the chosen sources, and this can employ qualitative or quantitative techniques. For this study, a qualitative content analysis was used for the initial analysis of the 46 articles, of which 31 were chosen for final inclusion in the study. This was done in the preparation step of the qualitative content analysis. These articles were further analysed for the purpose of categorization. The categories that were identified were information security, PHR-specific risks, cloud-based risks, privacy and security, and information security risks. This categorization helped to organize the articles for better readability and also to structure the content of the chapter when reporting on the results. This was done in the organization step of the qualitative content analysis. Finally the results were reported on in this chapter. This was done in the reporting stage of the qualitative content analysis.

This section described the research process that was followed in order to obtain content for this chapter. The next section describes the concept of information security.

3.3. Information security

This section highlights the importance of protecting information; it provides some background on information security, and discusses its definition and related aspects. It also describes the process of risk analysis, i.e. its components and the process to be followed.

Information is what keeps organisations functional. It is the life blood of every business; and whether it involves confidential information or the day-to-day running of the business, it needs to be protected (Gordon, 2002; Peltier, 2016). Information can be grouped into different categories, depending on its importance, sensitivity, and vulnerability to theft or misuse (Rhodes-Ousley, 2013). For instance, it can be classified as personal – meaning it is not owned by the organization keeping it, but by a private individual. It can also be public, i.e. intended for distribution to and viewing by the general public. Information can be confidential. This means that it can only be used by employees, contractors and business partners. It can also be proprietary, meaning it is intellectual property that belongs to the organization, and can only be handled by the authorized parties. Finally, information can be classified as secret. This means it is for use by entitled people only, those with a need to know (Rhodes-Ousley, 2013).

The protection of information is mandatory – and not just desirable (Rhodes-Ousley, 2013). The loss or theft of confidential information has the potential of damaging an individual's privacy; but it can also cause damage to the company that was handling the information (Rhodes-Ousley, 2013). Information is prone to a number of risks, and more specifically, security risks. Organisations that are custodians of sensitive information need to perform a risk analysis; in order to ultimately defend themselves against the threat of being identified (Elky, 2006; Rhodes-Ousley, 2013).

The identified information security risks then need to be mitigated. The mitigation of risks does not necessarily mean they will be eliminated; it is just a means of reducing them to an acceptable level (Rhodes-Ousley, 2013).

The **Information Systems Audit and Control Association** (ISACA, 2012, p. 19) defines information security as something that "ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when this is required (availability)”.

According to ISACA (2012), information security involves the following three security services:

- **<u>C</u>onfidentiality**: The protection of privacy and proprietary information i.e. restricting access to and disclosure of sensitive information.
- **<u>I</u>ntegrity**: Guarding against improper modification or destruction of information, which includes non-repudiation and authenticity.
- **<u>A</u>vailability**: Ensuring that information is accessible in a timely and reliable fashion.

Collectively, these are known as the information security services or the CIA triad. Now that information security has been introduced; the next subsection will discuss the concept of risk assessment; as this is an important process in managing risk. Risk assessment is discussed in this study, in order to help create an understanding of the terms used. It should be noted that the risk assessment process does not form part of the output (guidelines) of the study.

3.2.1 Risk Assessment

Risk management involves recognising the risk, assessing it, and taking measures to reduce it (Nikolić & Ružić-Dimitrijević, 2009; Sadgrove, 2016). This is important, in order to protect the mission and the assets of an organisation (Elky, 2006). The ISO 27005:2011 document defines risk as an “effect of uncertainty of objectives” (International Organization for Standardization, 2011). Information security risk is usually expressed in terms of a combination of the consequences of an information security event and the associated likelihood of it happening (International Organization for Standardization, 2011).

According to the ISO standard on Information technology – security technique – information security risk management (International Organization for Standardization, 2011), risk assessment is a process that consists of the following activities:

- **Risk Identification**: The purpose of this step is to determine what could happen that would cause a potential loss, and to also get a perception of where and why the loss might occur. The steps involved in this activity are listed below:
    - Identification of assets
    - Identification of threats
    - Identification of existing controls
    - Identification of vulnerabilities
    - Identification of consequences

All the above steps feed into the next activity, which is:

- **Risk analysis**: This is the process of identifying assets within the security perimeter, identifying threats to those assets, determining the vulnerability of asset(s) to threat(s), determining the realistic probability of each threat/vulnerability combination, the calculation of harm/impact, and the calculation of risk (Carlson, 2001; Clinch, 2009; Krutz & Vines, 2010). Risk analysis can be qualitative or quantitative.
    - The qualitative approach assigns a severity-level scale to describe the potential consequences (e.g. Low, Medium, or High) and the likelihood of those consequences happening. This would help in prioritizing the remediation (Rhodes-Ousley, 2013).
    - The quantitative approach uses a numerical scale to measure both the consequences and the likelihood of the risk (Nikolić & Ružić-Dimitrijević, 2009).

The steps involved in risk analysis are:

- Assessment of the consequences
- Assessment of the incident's likelihood
- Level of risk determination

These steps can be represented by using a Matrix, as seen in Table 3.1:

Table 3.1: Risk analysis (International Organization for Standardization, 2011)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

The Matrix above represents a mapping of the likelihood of an incident scenario against the estimated business impact. The likelihood of an incident scenario is given by a threat exploiting a vulnerability within a certain likelihood. The resulting risk is measured on a scale of 0-8 that can be evaluated against the risk-acceptance criteria (see next activity).

The final activity is:

- **Risk evaluation**: This uses the list of risks obtained in the above activity, with the value levels assigned, and the risk evaluation criteria. This activity assists in making decisions about future actions.

This section has discussed the concept of information security, in order to highlight the importance of information, and also to highlight the importance of protecting it. The risk assessment process has been described in detail, in order to clarify the terms used in this document – and not to perform risk analysis. The next section will describe the information security risks that can be expected when storing information in the cloud.

3.4. Cloud-based information security risks

This section starts by highlighting the security risks associated with the use of the internet in general; and thereafter, it discusses those risks that relate specifically to cloud computing. This is done, in order to give a background on the general internet risks, of which users should always be aware. The cloud computing risks are then categorised, according to the information security services; and they are also discussed in such a way that they can be related to the use of PHRs.

Since cloud computing is part of the internet, the information security risks that come with it are not completely new. The internet already has risks that cause people to be sceptical about its use for storing sensitive information. These risks generally include, but are not limited to, the list below:

- **Phishing** – An attacker uses spam email, in order to trick credulous victims into providing critical information like passwords and account information, etc. (Barnett, 2011; Lareau, 2006; Rhodes-Ousley, 2013).
- **Password guessing** – Attackers use software to generate a list of possible passwords (Harris & Hunt, 1999; D. Wang, Zhang, Wang, Yan, & Huang, 2016).
- **Malware** – This refers to malicious software that is injected into a computer or other information systems (Lareau, 2006).
- **Virus** – This is a type of malware that self-replicates, when activated, and is able to attach copies of itself to nearby executable files in the computer (Lareau, 2006).
- **Information destruction** – An attacker sometimes invades a computer or information system with the intention of destroying the information contained in it (Harris & Hunt, 1999).

The risks above are general internet risks. However, cloud computing raises greater concern among people than does general internet use – because of the nature of cloud computing, and how information is stored and processed (see Chapter 2). The information security risks that pertain specifically to cloud computing will be discussed next.

3.3.1 Malicious insiders

When a PHR provider uses the cloud to store health data, he/she transfers trust to the provider of the cloud storage service. The CSP's staff members then have access to the PHR data; and they may misuse their access rights to perform malicious attacks on the PHR users' data (Behl, 2011; Zibouh, Dalli, & Drissi, 2016). Malicious insiders can be categorised into the following groups:

- **Rogue administrator:** This type of insider could be an administrator employed by the CSP, to back up and maintain their customer data (Mahajan & Sharma, 2015). The rogue administrator could then use this access to hurt the CSP or its customers (Claycomb & Nicoll, 2012). This category of malicious insider can also be referred to as a third party, which will be defined more accurately further down in the document.
- **Disgruntled employee:** This attacker targets his own employer, in other words, the CSP. They use the cloud as a tool to carry out attacks on systems or data stored by the CSP (Claycomb & Nicoll, 2012; Mahajan & Sharma, 2015). This category of insider threat can also be present in the form of an employee who was fired; but still has active access rights to the system (Shiels & Valley, 2009).
- **Unintentional malicious insider:** An insider may be tricked by an outsider from a different organisation into performing an attack on the system of the former's employer. It is, in fact, a sabotage attack to expose the company's sensitive or embarrassing information (Claycomb & Nicoll, 2012).

3.3.2 Third-party access

The cloud-based PHR provider may also transfer some duties, such as the administration of the data, to a third-party, who then creates a bigger pool of people who have access to the PHR data. The PHR user has no control over who sees his data, and what they do with it, hence increasing the fear of unauthorised access to the user's PHR (Modi, Patel, Borisaniya, Patel, & Rajarajan, 2013; Zissis & Lekkas, 2012).

3.3.3 Multi-tenancy

In cloud computing, users share resources, such as the Central Processing Unit (CPU), memory, networking capabilities, etc. This grants them direct access to the resources used by other users; because they use the same host machine. This raises the threat of attackers posing as PHR users, in order to gain access to other users' PHRs (Liu, Huang, & Liu, 2015; Mishra, Mathur, Jain, & Rathore, 2011).

3.3.4 Software intrusions

A user's PHR data may be compromised through an injection of malicious software, e.g. a virus, which the attacker may then use to gain sensitive information, such as the log-in credentials of the user. Phishing may also be used to this end (Wei, Pu, Rozas, Rajan, & Zhu, 2013).

3.3.5 Physical intrusions

Cloud computing uses data centres to store the users' data. These are at a risk of being attacked physically; and such an attack may lead to hardware theft and/or unauthorised access to servers. Intruders may also have the intention of destroying the information *via* an information destruction attack (Hutchings, Smith, & James, 2013).

3.3.6 Poor encryption key management

Users may be allowed to create their own decryption keys, and to distribute them as they see fit. If the keys fall into the wrong hands, the user's PHR data may be at risk. There is also a chance of password cracking, to which the PHR data may be vulnerable if the encryption key management techniques are not of a good standard (AbuKhousa et al., 2012; Kuo, 2011).

3.3.7 Temporary outages

Even though cloud computing is known for its high level of service reliability and availability, it can and does experience outages (AbuKhousa et al., 2012; W. Jansen & Grance, 2011). Cloud services experience outages, which may last for hours, thereby prohibiting access to PHR data.

3.3.8 Permanent and prolonged outages

A CSP may experience serious problems that could lead to bankruptcy or facility loss (Gunawi et al., 2016; W. Jansen & Grance, 2011). This affects access to the users' PHRs for extended periods; and sometimes, it even leads to the CSP's complete shutdown (W. A. Jansen, 2011).

3.3.9 Data lock-in

This is the inability of customers to move their data from one provider to the next, due to (for example) the current provider running out of business (Alex Mu-hsing Kuo, 2011; Sai & Gupta, 2015). A PHR may need to be moved from one storage facility to another – for various reasons. Cloud computing makes this difficult, because most cloud infrastructures have little capability with respect to their interoperability (W. A. Jansen, 2011).

3.3.10 Denial of Service (DoS)

This is performed by "saturating the target with bogus requests, in order to prevent it from responding to legitimate requests in a timely manner" (W. A. Jansen, 2011). The attacker then prevents the PHR from processing any real requests from the users (Win, Susilo, & Mu, 2006).

Security and privacy risks that could affect customers who use a cloud-based PHR have already been discussed above. The risks were discussed in detail, giving insight into their nature, and how they relate to cloud-based PHRs. Appropriate control measures that can reduce the risks to an acceptable level need to be identified and implemented. The following chapter proposes guidelines that can be used to mitigate these risks, while helping PHR providers to choose a secure CSP.

3.4. Conclusion

This chapter has provided some background on the three security services of information security. This was necessary, in order to categorise the identified information security risks. Cloud-based information security risks were identified and discussed. This chapter’s output helped to meet the fulfilment of the secondary objective: “Identify information security risks, of which PHR providers should be aware, when storing their customers’ data in the cloud.” This will feed into the content for the following chapter. Chapter 4 provides the formulation of guidelines that can assist a PHR provider when selecting a CSP.

Chapter 4- Formulation of guidelines for secure cloud-based Personal Health Records

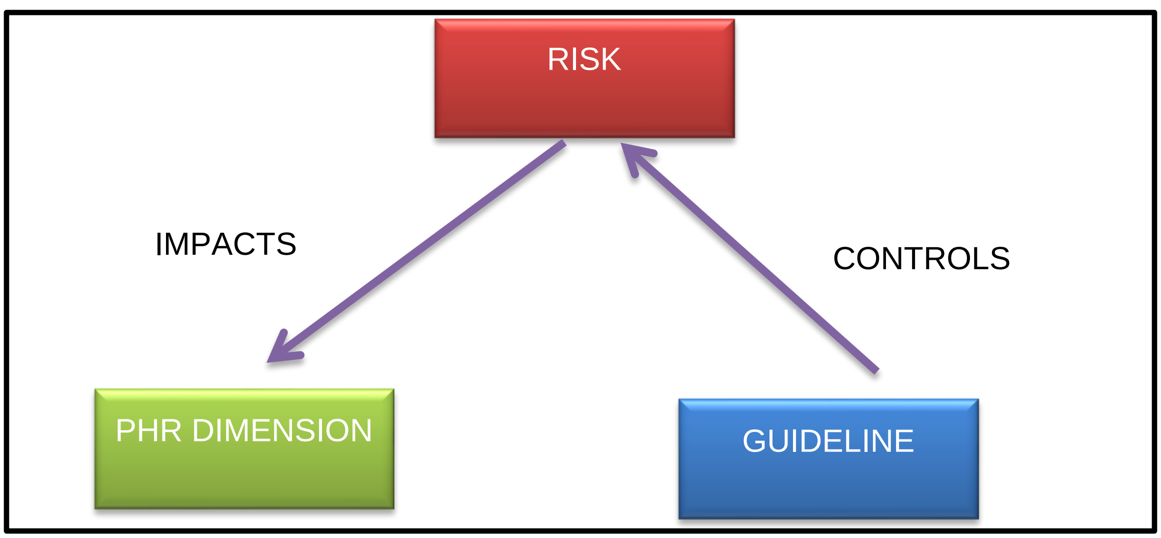
Chapter Content

CHAPTER 4: FORMULATION OF GUIDELINES FOR SECURE CLOUD-BASED PERSONAL HEALTH RECORDS

4.1 Introduction

The information security risks that were identified in Chapter 3 are here discussed in terms of the PHR dimensions discussed in Chapter 2. Guidelines that can help control these information security risks are subsequently formulated in this chapter (Chapter 4). These guidelines were developed for each of the information security risks, in order to maintain the integrity of the PHR dimensions. Figure 4.1 illustrates how an information security risk can have an impact on a PHR dimension, and how a guideline can be used to control each risk.

Figure 4.1: Relationship between information security risks, PHR dimensions, and guidelines



4.2 Information security risks that have an impact on PHR dimensions

As mentioned in Chapter 2, a PHR has to satisfy certain requirements, as it relates to the following nine (9) dimensions, in order to be deemed useful (van der Westhuizen, 2010):

- Confidentiality
- Integrity
- Availability
- Auditability
- Accuracy
- Completeness
- Apomediation
- Privacy
- Interoperability

In this section, the information security risks that affect the above PHR dimensions are discussed. This discussion follows the context in which van der Westhuizen (2010) presented these dimensions. However, some of the PHR dimensions were found to be irrelevant in terms of potential information security risks. The motivation for this decision is as follows. Information security focuses on three states of information: when information is at rest i.e. stored in a file somewhere; in transit, i.e. moving from one location to the other; or in use i.e. actively open and used by an application or user (Rhodes-Ousley, 2013). The PHR dimensions, that are therefore affected by information security risks relate to the use or access of information while it is in one of these three states. Thus, it can be argued that the information in the PHR dimensions below is not in either one of the mentioned states. Therefore, there are no information security risks that affect this information. Consequently the three PHR dimensions, namely completeness, apomediation and accuracy were excluded.

Completeness in the context of the PHR dimensions pertains to capturing relevant information about the health of the patient, such as basic personal information, diagnosis details, allergies, and so forth (van der Westhuizen, 2010). This dimension relates to the functionality offered by the PHR – in other words, whether it allows a user to capture enough detail to accurately represent his health history. Since this dimension does not relate to the availability of the information captured in the PHR, but rather involves the option to capture the information; there are no information security risks associated with this dimension. ISACA describes information completeness as “the extent to which information is not missing and is of sufficient depth and breadth for the task at hand” (ISACA, 2013, pg 2). This means that all the required information to complete an action should be available. This does not relate to Completeness as described from the perspective of a PHR dimension, which merely relates to data capturing, therefore this was excluded from the dimensions affected by information security risks.

Apomediation is the ability of a PHR to educate individuals about health matters and to assist them in interacting with their physicians via the PHR (van der Westhuizen, 2010). It is formally described as “ the term used to describe using a person who facilitates your pursuit of information on the Internet” (Torrey, 2016, para 1). A PHR is linked to tools such as blogs and wikis etc. that assist a PHR user to better understand medical terms and thus capture information more accurately (van der Westhuizen, 2010) . There are, therefore, no information security risks that can have an impact on the PHR in this dimension. Similar to the ‘completeness’ dimension, this dimension rather relates to the functionality offered by a PHR.

Accuracy is ensuring that the information captured on the PHR is a true reflection of the original paper-based health record or diagnosis obtained from the healthcare provider (van der Westhuizen, 2010). As per the accuracy dimension, a PHR should be able to prevent human error whenever an individual captures health information on the system, and/or implements various error-checking tools to ensure accurate data-capturing. This dimension again refers to the functionality included in the PHR to ensure accuracy and as such there are no information security risks associated with it. In terms of information security literature, the term ‘accuracy’ refers to the need to ensure that information is not tampered with in order to ensure the correctness and reliability of information (ISACA, 2013).

The PHR dimensions that are affected by the information security risks are:

- Confidentiality
- Integrity
- Availability
- Auditability
- Privacy
- Interoperability

Table 4.1 illustrates those information security risks, as they were identified in Chapter 3, which may have an impact on the relevant PHR dimensions. Chapter 3 identified general internet risks as well; but these were not included as information security risks in this chapter; because most of them are already incorporated in the cloud-based information security risks. In order to link each risk factor to a dimension, the requirements related to each dimension were considered, in order to determine which risk factor(s) would have a negative impact on it. Looking at the risks, one is able to find a link that demonstrates how a dimension may be affected negatively, should such a risk factor prevail.

Table 4.1: Information security risks versus PHR dimensions

RISKS	PHR DIMENSIONS					
	Confidentiality	Integrity	Availability	Auditability	Privacy	Interoperability
Malicious insiders	✓	✓	✓	✓	✓	
Third-party access	✓	✓	✓	✓	✓	
Multi-tenancy	✓	✓	✓		✓	
Software intrusion	✓		✓		✓	
Physical intrusion	✓	✓	✓		✓	
Poor encryption key management	✓		✓		✓	
Temporary outages			✓			
Prolonged and permanent outages			✓			
Data lock-in						✓
Denial of Service (DoS)			✓			

The following subsections describe the information security risks, according to the PHR dimensions on which they have an impact, as illustrated in Table 4.2. Examples will also be provided to clearly demonstrate the impact that the risks have on the dimensions, and ultimately on the security of the PHR. Each subsection, further lists the PHR dimension on which the information security risks have an impact, together with an explanation of each, and an example of where each of these is applicable/possible.

4.2.1. Malicious insiders

The staff members of a CSP may abuse their access to a PHR, in order to perform malicious attacks. The threat of malicious insiders is amplified in cloud computing because of how information technology services and customers are all in one management domain (Mahajan & Sharma, 2015). The fact that the insider has more than enough time to study and understand the CSP's system, makes it difficult to predict and detect the threat in time (Modi et al., 2013).

Below is a list of the dimensions that are affected by this risk; and where possible, examples are given for each dimension, in order to emphasise how malicious insiders pose a risk to the PHR data.

- **Confidentiality** – The confidentiality of a PHR can be compromised if the data are somehow leaked, or if there is a misapplication of the network rights. A malicious insider may gain access to sensitive information stored in the cloud, in order to sell it or sabotage the company (Claycomb & Nicoll, 2012). This type of breach is hard to detect; because the person already has direct access to the system (Modi et al., 2013).
- **Integrity** – The integrity of a cloud-based PHR may be compromised when a malicious insider with authorised access makes unauthorised modifications to the PHR – or even to the software applications in the cloud. A disgruntled employee may intentionally modify a program, when certain conditions are met, or during a certain period of time (Zissis & Lekkas, 2012).
- **Availability** – The availability of PHR data can be compromised if the first two aspects of the CIA triad are compromised. Hence, if confidentiality and integrity have been compromised, it implies that a third party gained unauthorised access; and by modifying the data, their availability may have been influenced.

- **Auditability** – It is vital that PHR systems should adhere to auditability for as long as the information is stored in them (Fernández-Alemán, Señor, Lozoya, & Toval, 2013). A system's audit can be defined as a one-time or periodic occurrence to assess security (Krutz & Vines, 2010). A disgruntled employee may launch a distributed denial-of-service attack on his organisation, in order to obstruct an audit and limit a forensic analysis of his malicious activities (Claycomb & Nicoll, 2012).
- **Privacy** – Data security and privacy are recognised as major concerns for PHRs (Kharrazi, Chisholm, VanNasdale, & Thompson, 2012). When individuals are unsure why their personal information is requested, who has access to it, and how it will be used, they develop trust issues (Pearson & Benameur, 2010). This lack of trust can be a key inhibitor to the adoption of cloud services, especially when it comes to processing confidential or sensitive information, such as health information. There is much legal uncertainty about privacy rights in the cloud, as privacy laws vary, according to the jurisdiction in which the information resides at a particular time, when stored in the cloud (Pearson & Benameur, 2010). The privacy challenge for software engineers of cloud services is to design the services in such a manner that decreases privacy risks, and ensures legal compliance (Ramgovind, Eloff, & Smith, 2010). It is possible for a malicious insider to knowingly access and release patients' sensitive health information to outsiders – out of spite or revenge. And this is a serious violation of privacy.

4.2.2. Third-party access

The CSP may outsource some functions, like storage, to a third party. This automatically creates a greater pool of people who have access to the users' PHR system. The dimensions affected by this risk are described next; and some examples will also be given for each, in order to emphasise how third-party access can pose a risk to PHR data:

- **Confidentiality:** A third party acting as a rogue administrator may access the servers of the CSPs and gain access to the customers' PHRs. An example of such an attack is that of a system administrator of a data-mining firm that used to have access to the servers and to the data that belonged to the victim organisation. The attacker downloaded millions of personal records that belonged to the customers of the victim organisation (Claycomb & Nicoll, 2012). This type of attack compromises the confidentiality of information; and it could easily happen to a CSP that is storing PHRs.
- **Integrity:** One needs to be sure that information has not been altered in any way throughout the capture, storage and communication process. The integrity of such information may be compromised by a third party that decides to modify the contents of the PHR, without being granted permission to do so by the owner. A certain cell-phone provider that stored customers' data in a Microsoft subsidiary cloud was unavailable when the provider lost the data. Thus, the level of data integrity was not guaranteed, should those data be restored (Paquette, Jaeger, & Wilson, 2010).
- **Availability:** It is possible that the third party that stores PHR data may be unavailable – for many reasons. In 2008, it was reported that a CSP ceased operation without giving adequate notice to its customers. It was further reported that 45% of the data's safety were not guaranteed, in terms of it being available or being restored (Paquette et al., 2010). If such a provider is a third party that stores PHR data, this could lead to problems with the care of a patient; since his health record would cease to exist. The third party may also decide to hold the data hostage, if there is a dispute with the CSP (Ashktorab & Taghizadeh, 2012).
- **Auditability:** An audit can be performed by internal or external auditors; and it can be the responsibility of the CSP, the customer or even both. When the CSP outsources some services to a third party, auditing may be difficult; because some functions may not be transparent enough for inspection (Choubey, Dubey, & Bhattacharjee, 2011).

- **Privacy:** The third party that stores the CSP's data may store them anywhere in the world. This raises privacy concerns for cloud-based PHRs; because the PHR owners would not necessarily know where their data are being stored. Different privacy laws apply for different jurisdictions; so it may be difficult to access data or move them from one country to another (Subashini & Kavitha, 2011).

4.2.3. Multi-tenancy

The nature of cloud computing allows different customers to share resources, such as storage and processing; and this creates an opportunity for malicious users to gain access to other users' data (Subashini & Kavitha, 2011). Below are the dimensions affected by this risk, as well as some examples for each, in order to emphasise how multi-tenancy poses a risk to PHR data:

- **Confidentiality:** Protected data may be exposed to an adversary; hence, compromising confidentiality. A pertinent example is that of a cloud user that reads another user's workflow without permission (Saripalli & Walters, 2010). This may also happen to someone's PHR data.
- **Integrity:** An adversary can gain access to a PHR via the multi-tenant environment and perform unauthorised changes to the data, thus affecting their integrity (Carroll, Van Der Merwe, & Kotzé, 2011).
- **Availability:** Service and data availability are vital for healthcare providers who use cloud applications to access their patients' data (AbuKhousa et al., 2012).
- **Privacy:** Data stored in the cloud are accessible to other users because of the sharing of resources. The PHR data may be accessed by an unauthorised user; and this raises a privacy threat that may lead to medical identity theft, private medical data being made available to unauthorised parties, and so forth (Adhikari, Richards, & Scott, 2014).

4.2.4. Software intrusions

The cloud environment is prone to malicious software attacks due to the fact that it is hosted on the web (Singh, 2014). The PHR dimensions affected by this risk are listed below, together with examples for each, in order to emphasise how software intrusions pose a risk to PHR data:

- **Confidentiality:** Unauthorised access to the cloud environment may affect the confidentiality of the data contained therein. An example is given of an outside attacker that gained access to an organisation's system by obtaining the credentials of one of the employees. The attacker gained access by tricking the employee into opening a document infected with malware, which gave him access to the organisation's email service (Claycomb & Nicoll, 2012).
- **Availability:** The cloud is vulnerable to zombie attacks. An attacker tries to bombard the victim by sending requests from innocent hosts (zombies) in the network. This type of attack may interrupt the expected behaviour of the cloud, which affects availability (Modi et al., 2013). Availability is crucial for PHR applications.
- **Privacy:** Phishing is used to trick users into exposing their data by manipulating them to click on a false link that redirects from the page they were currently accessing. It is possible in the cloud environment to hijack the accounts and services of cloud users; and thus to expose sensitive data that should not be revealed (Modi et al., 2013).

4.2.5. Physical intrusions

Cloud computing services can be disrupted by threats caused by unauthorised physical access to the data centres where the data are stored (Paquette et al., 2010). The PHR dimensions affected by this risk are listed below:

- **Confidentiality:** Data theft in the cloud data centre may lead to a breach in confidentiality; as the information contained there may be accessed by unauthorised individuals (Kumar, Akash, Somesh, & Dewangan, 2013).

- **Integrity:** It is vital to ensure that the physical data centres that store cloud data are protected from theft, modification and fabrication. This extends to the network architecture through which the data travel. Network attacks pose a threat not only to the traffic coming towards the cloud, but also to that between cloud hosts (Singh & Pandey, 2013).
- **Availability:** This refers to data, software and also hardware resources being available to authorised users when needed (Zissis & Lekkas, 2012). Hardware theft of cloud resources has a huge impact on the efficiency and productivity of cloud services (Singh & Pandey, 2013); as it may lead to a loss of both the data and the hardware.
- **Privacy:** The storage of cloud data at remote third-party data centres gives rise to security issues, such as privacy breaches (Subashini & Kavitha, 2011). The CSP that stores the PHR data may well have full control over them, thus allowing privacy violation (Kumar et al., 2013).

4.2.6. Poor encryption key management

Users of cloud services have the option to encrypt their own data (AbuKhousa et al., 2012); and therefore, there is the possibility of the disclosure or loss of the encryption keys. The PHR dimensions affected by the risk of poor encryption key management are listed below:

- **Confidentiality:** Using a single key to encrypt data and sharing the key with the different parties that have access to the data may cause confidentiality problems. A malicious or compromised cloud user may gain access to the key by pretending to be a legitimate user (Puttaswamy & Zhao, 2011).
- **Availability:** Data in the cloud reside in a shared environment; and multi-tenancy and service providers all have access to it. Inadequate encryption or poor management of the encryption keys may lead to data loss, and unavailability of the data when needed (Carroll et al., 2011).
- **Privacy:** Ideally, it is the data owners who are responsible for key management; but if the users of cloud services do not have adequate

expertise to manage their encryption keys, they may entrust their CSPs to perform this task (Chen & Zhao, 2012). This may raise privacy concerns; because it means the CSP has unlimited access to private information and may compromise it.

4.2.7. Temporary outages

Even though cloud computing is known for its high level of service reliability and availability, it can and does experience outages (Leavitt, 2009). The PHR dimension affected by this risk is given below, together with examples of each, in order to emphasise how temporary outages can pose a risk to PHR data:

- **Availability:** In 2008, a temporary outage was witnessed in the three-hour outage that affected Amazon's Simple Storage Service. This consequently affected Twitter and other companies using the service. Cloud services may also be affected by connectivity and bandwidth-speed limitations. PHR data need to be accessible at all times, especially during emergency situations. An outage may affect the care of a patient (W. A. Jansen, 2011).

4.2.8. Prolonged and permanent outages

A CSP may experience problems, such as bankruptcy or facility loss, which may lead to the unavailability of services for extended periods, if not forever (W. A. Jansen, 2011). The PHR dimension affected by this risk is given next, together with an example, in order to emphasise how prolonged and permanent outages can pose a risk to PHR data:

- **Availability:** In 2008, an online storage provider named Omnidrive closed down – without warning its users. This affected the availability of the data with that provider (W. A. Jansen, 2011). Patients need to always have a record of their health data. Losing a PHR means losing a lifetime of information; as it is collected over a long period of time.

4.2.9. Data lock-in

Data lock-in is caused by the loss of portability of the customer's data and programs (Tripathi & Mishra, 2011). The PHR dimension affected by this risk is given below, together with an example, in order to emphasise how data lock-in poses a risk to PHR data:

- **Interoperability:** If the current CSP runs out of business while storing customer data, customers are not able to retrieve their data and move such to another provider (Tripathi & Mishra, 2011). When Google Health was discontinued in January 2012, its users had a year to download their health data. However, most infrastructures in the cloud do not support interoperability between their data, applications and services. This makes it difficult to move the PHR data to another provider or in-house IT environment (Kuo, 2011).

4.2.10. Denial of Service (DoS)

This occurs when an attacker sends bogus requests to the server to cause an overflow that would block legitimate requests from reaching the server – thus making its services unavailable (W. A. Jansen, 2011). The PHR dimension affected by this risk is given below, together with an example, in order to emphasise how data lock-in poses a risk to PHR data:

- **Availability:** An example in this regard is that of a code-hosting site called BitBucket, which had an outage for over 19 hours, due to a DoS attack on the Amazon infrastructure that it uses (Modi et al., 2013). Depending on the extent to which a patient is reliant on PHR data, the loss of availability may have a huge impact.

The above section revisited the PHR dimensions discussed in Chapter 2, in order to demonstrate their relationship with the information security risks identified in Chapter 3. The following section revisits the risks discussed thus far; and it also introduces the guidelines that can be used to control each of these.

4.3 Guidelines for secure cloud-based PHRs

This section proposes guidelines that can be used to mitigate the risks discussed in Section 4.2. Information security plays a role in ensuring that sensitive information – in this case, personal health information – is treated with the utmost care and protection. The ISO 27799:2008 standard for information security management in health (International Organization for Standardization, 2008), together with ISO 17090-3:2008 policy management of certification authority (International Organization for Standardization, 2009), was consulted – in order to identify control measures that could potentially protect the security of cloud-based PHRs. The section is structured, according to the risks, to show which guideline would be applicable for each risk. Section 4.2 also contains a discussion on PHR dimensions; and how each risk affects each dimension. Each of the guidelines will thus be presented and followed up by a brief conclusion for each – on how the application of the guideline would ensure that the PHR dimensions are preserved.

Table 4.2 below presents a summary of the guidelines that can be employed to control each risk. The sources that were consulted, in order to identify the relevant control measures for the risks, are also presented in Table 4.2. A discussion of the guidelines will be presented below the table.

Table 4.2: Guidelines for secure cloud-based PHRs versus the risks

Risk	Guideline	Control Measures (ISO 27799:2008*, ISO 27017:2015 $& ISO 17090-3:2008#)	Source
Malicious insiders	• Control access to PHR data	• Access control policy (7.8.1.2)* • Access to networks and network services (9.1.2) $ • Roles and responsibilities; Screening; Terms and conditions of employment (7.5.1)* • Management responsibilities; Information security awareness, education and training; Disciplinary process (7.5.2)* • Terminating responsibilities and return of assets; Removal of access rights (7.5.3)* • User registration and deregistration (9.2.1) $ • Information access restriction (9.4.1) $	• Behl, 2011
Third-party access	• Assess risks involved with third parties	• Assessment of risks related to external parties (7.3.3.1)* • Addressing security in third-party agreements (7.3.3.3)* • User access provisioning (9.2.2) $ • Management of privileged access rights (9.2.3) $ • Health information exchange policies and procedures and exchange agreements (7.7.8.1)*	• Modi et al., 2013 • Sengupta, Kaulgud, & Sharma, 2011
Multi-tenancy	• Separate customer data	• Separation of development, test and operational facilities (7.7.1.4)* • Separation of development, testing and operational environments (12.1.4) $ • Segregation in networks (13.1.3) $	• Mishra et al., 2011 • Modi et al., 2013
Software intrusion	• Prevent malicious code infections	• Controls against malicious code (7.7.4.1)* • Controls against malware (12.2.1) $	• Mahmood & Hill, 2011 • Wei et al., 2013
Physical intrusion	• Store PHR data in secure data centres	• Physical security perimeter (7.6.1.1)*, (11.1.1) $ • Physical entry controls (11.1.2) $	• Hutchings et al., 2013
Poor encryption key management	• Adopt strong private key management techniques	• Policy on use of cryptographic controls (10.1.1) $ • Key management (10.1.2) $ • Private key backup (7.6.2.5) # • Method of destroying private key (7.6.2.11) # • Avoid loss, disclosure or unauthorised use of private keys. If any occurs, report immediately (7.9.6.4) #	• AbuKhousa et al., 2012; • Alex Mu-hsing Kuo, 2011
Temporary outages	• Ensure business continuity • Consider loss of network impact	• Information security aspects of business continuity management (disaster recovery) (7.11)* • Security of network services (7.7.6.2)* • Alignment of security management for virtual and physical networks (CLD.13.1.4) $ • Administrator's operational security (CLD.12.1.5) $	• AbuKhousa et al., 2012 • Fernández-Cardeñosa, De La Torre-Díez, López-Coronado, & Rodrigues, 2012 • Onwubiko, Rimal, Choi, & Lumb, 2010

Continuation of Table 4.2

Risk	Guideline	Control Measures (ISO 27799:2008*, ISO 27017:2015 $ & ISO 17090-3:2008#)	Source
Prolonged and permanent outages	• Back-up and encrypt PHR data	• Health information back-up (7.7.5)* • Information back-up (12.3.1) $	• Jansen & Grance, 2011
Data lock-in	• Enforce technical interoperability	• Compliance with security policies, standards and technical compliance (7.12.3)*	• Carroll et al., 2011 • Dillon, Wu, & Chang, 2010
Denial of Service (DoS)	• Report security incidents	• Reporting information security events and weaknesses (7.10.1)* • Reporting information security events (16.1.2)$	• AbuKhousa et al., 2012 • Carroll et al., 2011 • Modi et al., 2013

* denotes the use of the ISO 27799:2008 standard

$ denotes the use of the ISO 27017:2015 standard

# denotes the use of the ISO 17090:2008 standard

4.3.1. Malicious insiders

The insider threat is very common in the cloud environment; and there is usually a lack of transparency on the hiring process of the CSP. There is no clarity about their hiring standards and practices, and this creates an opportunity for an opponent to gain access to sensitive information (Behl, 2011). The main guideline that has been identified to limit this risk is to **control access to PHR data**, which implies the following:

- In order to govern access to personal health information, an access control policy should be in place. It should be predefined, according to the roles with associated authorities, which are consistent, but limited to the needs of that particular role (7.8.1.2).
- The PHR provider's access control policy, which provides guidance on the use of network services, should specify requirements for user access to each separate cloud service that is provided by the CSP (9.1.2).
- Prior to employment, staff members should be given roles and responsibilities in the job description. A screening process should also be conducted to verify identity, living address, previous employment, as well as the terms and conditions of employment (7.5.1).
- During employment, staff members should be assigned responsibilities, offered information security awareness and training, and be informed of the disciplinary process (7.5.2).
- Upon termination or change of employment, access rights must be revoked (7.5.3)
- The CSP should provide user registration and deregistration functions for the customers of the PHR provider. The specifications of how these functions work should also be provided to the PHR provider (9.2.1).
- The CSP should provide access controls that allow PHR providers to restrict access to their cloud services, their cloud service functions and the PHR provider's data maintained in the service (9.4.1).

Implementing this guideline would ensure that the confidentiality of a PHR is preserved. Employees of the CSP will be governed by a control policy that will clearly state the role of each employee and the type of access he/she has. This would also protect the integrity of the data, because any employee who makes changes to the data, without having the proper access rights, would be held liable. Employees who are no longer with the CSP should have their access rights revoked; so as to prevent them from tampering with the availability, auditability and privacy of the PHR data.

4.3.2. Third-party access

Adding more administrators to cloud systems increases the risk of unauthorised access (Modi et al., 2013). The third party may pose a threat to the users of cloud services if he/she aims to use such access in a negative way. Other risks involved with third parties include maintaining data confidentiality and integrity (Sengupta et al., 2011). The guideline that has been identified to limit this risk is to **assess the risks involved with third parties**, which implies the following:

- Organisations that are responsible for processing health information must conduct a risk assessment, in order to assess the risks that may be brought by third parties to the systems and data. Security controls must subsequently be implemented, according to the identified level of risk and to the technologies used (7.3.3.1).
- Where a third party is granted access to process personal health information, there must be formal contracts that specify the confidential nature and value of the personal health information; the security measures that must be implemented and complied with; limitations to access these services by third parties; and the penalty that would be applicable, should any of these be breached (7.3.3.3).
- The CSP should support third-party identity and access management technologies for its cloud services and associated administration interfaces (9.2.2).
- The CSP should provide sufficient authentication techniques for authenticating the PHR provider's administrators to the administrative capabilities of a cloud service, according to the identified risks (e.g. enable the use of third-party multi-factor authentication mechanisms) (9.2.3).
- Information exchange agreements that specify the minimum set of controls to be implemented must also be formulated (7.7.8.1).

Third parties that have access to PHR data can be controlled in terms of the risks they may bring, should they perform malicious acts. The confidentiality, integrity, availability, auditability and privacy of PHRs can be well kept; if the risks that come with third parties are well-assessed and managed in good time.

4.3.3. Multi-tenancy

The lack of compartmentalisation of resources in cloud computing allows users to access other users' personal information (Mishra et al., 2011). Multi-tenancy also makes it difficult to monitor and log the processes of virtual machines in the cloud (Modi et al., 2013). The guideline that has been identified to deal with this risk is to **separate customer data**. This implies the following:

- Development, test and operation facilities should be separated physically or virtually (7.7.1.4).
- Development, testing and operational environments should be separated; so as to reduce the risks of unauthorized access or changes to the operational environment (12.1.4).
- The PHR provider should define the requirements for the segregation of networks, in order to achieve tenant isolation in the shared environment of a cloud service, and to ensure that the CSP meets those requirements (13.1.3).

In order for PHRs to retain their confidentiality, integrity, availability and privacy, customers' data should be separated.

4.3.4. Software intrusion

It is difficult to eliminate software vulnerabilities in the cloud; and this raises concerns for prospective cloud customers. Malware also compromises the integrity of software in the cloud; because it can somehow modify the victim's software (Mahmood & Hill, 2011). The guideline that has been identified to deal with this risk is to **prevent malicious code infections**. This implies the following:

- Proper prevention, detection and response controls that are used to protect systems against malicious software must be adopted; and appropriate user awareness and training must be implemented (7.7.4.1).
- Detection, prevention and recovery controls to protect against malware should be implemented, in conjunction with appropriate user awareness (12.2.1).

When PHRs are protected from software intrusions by preventing, detecting and properly responding to malicious code infections, the confidentiality, availability and privacy of PHRs would be preserved.

4.3.5. Physical intrusion

The data centres that CSPs use to store the PHR data may be at risk of being attacked physically, which would result in hardware theft, unauthorised access to servers, or loss of access to data (Hutchings et al., 2013). The guideline that has been identified to limit this risk is to **store PHR data in secure data centres**. This implies the following:

- A physical security perimeter should exist, in order to control access to facilities that contain personal health information. There should be physical entry controls; offices should be secured; there should be protection against external and environmental threats; and public access, delivery and loading areas should be secure enough not to endanger personal health information. These are all ways to prevent the public from getting too close to IT equipment. Software or equipment used to support a healthcare application that contains personal health information should not be removed from the site or relocated within the organisation – without authorised permission from the organisation (7.6.1.1).
- Security perimeters should be defined and used to protect areas that contain information that is either sensitive or critical (11.1.1).
- Secure areas should be protected by appropriate entry controls, to make sure that only people with authorized access are allowed entrance (11.1.2).

The confidentiality, integrity, availability and privacy of PHRs would be protected; if the data centres used to store the PHR data are kept secure from external and environmental threats.

4.3.6. Poor encryption key management

Some systems allow users to generate their own decryption keys and to distribute them to authorised parties (AbuKhousa et al., 2012). This becomes a challenge, if the user loses the keys, or discloses them to malicious parties (Kuo, 2011). For the purpose of the identified control measures, encryption keys are from this point onwards referred to as private keys; and the party responsible for keeping the keys is known as the certified holder. The guideline that has been identified to deal with this risk is to **adopt strong private key management techniques**. This implies the following:

- The CSP should provide information to the PHR provider about the circumstances in which it uses cryptography to protect the information it processes. The CSP should also let the PHR provider know if it can offer them any options that would allow the PHR provider to perform its own cryptographic protection (10.1.1).
- The PHR provider should not allow the CSP to store and manage the encryption keys for cryptographic operations, when it uses its own key management, or a separate and distinct key management service (10.1.2).
- It is recommended that the certificate holder creates a backup of the private keys, where possible. This backup would be held in the environment of the certificate holder and they would be entirely in his control (7.6.2.5).
- When the private key is no longer in use, all the copies in the computer memory and shared disk space must be securely destroyed – by overwriting multiple times (7.6.2.11).
- A certificate holder must ensure that he/she makes every effort to avoid the loss, disclosure or unauthorised use of his private keys. If there is any actual or suspected loss, disclosure or other compromising of the private key, the certificate holder must immediately notify the certification authority (7.9.6.4).

When encryption keys are managed and disposed of properly, the confidentiality, availability and privacy of PHR data can be ensured.

4.3.7. Temporary outages

It is vital that systems that process health information in the cloud should be available continuously without any interruptions (AbuKhousa et al., 2012). Outages are not exclusive to cloud environments; but they are highlighted there, because of the interconnectedness of their services (Gonzalez et al., 2011). A temporary outage could be caused by a natural disaster, vulnerability exploits and deliberate attacks (Onwubiko et al., 2010). The guideline that has been identified to limit this risk is to **ensure business continuity**. This implies the following:

- Health organisations recognise business continuity management as a requirement; and this would include disaster recovery (7.11).
- They should carefully consider what impact the loss of network service availability would have on a clinical practice (7.7.6.2).
- In a cloud computing environment, any inconsistency of network policies can cause system outages. The CSP should define and document an information security policy for the physical network (CLD.13.1.4).
- The PHR provider should create a document that contains procedures for critical operations; where failure could cause unrecoverable damage to the assets in the cloud computing environment. This document should specify that a supervisor should monitor such operations (CLD.12.1.5).

In case a PHR goes offline or is unavailable for any reason, business continuity should be ensured by considering the impact that this would have, and taking measures to avoid such a possibility.

4.3.8. Prolonged and permanent outages

When the cloud that is used for storage is unavailable for extended periods; this has a negative impact on the customer, who relies on the data. It is important for a CSP to have a plan for how the data would be recovered, and to ensure that it is still accessible

(W. Jansen & Grance, 2011). The guideline that has been identified to limit this risk is to **back up and encrypt PHR data**. And this implies the following:

- In order to make sure that personal health information would be available in future; it should be backed up and stored in a physically secure environment (7.7.5).
- In a case where the CSP provides back-up capabilities, as part of the cloud service, the PHR provider should request the specifications of the back-up capability (12.3.1).

PHR data should be backed up and encrypted to ensure their availability.

4.3.9. Data lock-in

It is possible for customer data to be locked in to the cloud for a number of reasons – such as the provider going out of business (Carroll et al., 2011). The lack of interoperability between cloud services prohibits customers from utilising multiple providers at the same time (Dillon et al., 2010). The guideline that has been identified to deal with this risk is to **enforce technical interoperability**, which implies the following:

- Systems that process personal health information need to be technically interoperable; as many of them typically consist of different interoperating systems (7.12.3).

It is vital for PHRs to be interoperable with other health systems, in order for them to be deemed useful.

4.3.10. Denial of Service (DoS)

Denial of Service (DoS) poses numerous threats in the cloud computing environment (Carroll et al., 2011). By attacking one server, the attacker might well affect the availability of other services as well (Modi et al., 2013). This threat is intensified in a health system that becomes unavailable, especially in an emergency situation (AbuKhousa et al., 2012). The guideline that has been identified to limit this risk is to **report security incidents**. This implies the following:

- Organisations that process personal health information should report security incidents. These include corruption or unintentional disclosure of personal health information, or the loss of availability of health information systems, where such a loss affects patient care in an undesirable manner (7.10.1).
- The CSP should have mechanisms in place that would allow the PHR provider to report any information security event to the CSP. The CSP should also report an information security event to the PHR provider, and should also keep track of the status of the reported information security event (16.1.2). The above section provided the guidelines that can be used to control the risk factors and ultimately assist PHR providers in selecting a secure CSP for their customers' data.

For PHRs to be kept available all the time, security incidents should be reported to the PHR providers, so that they can provide other means to keep the PHR accessible.

The above section provided the guidelines that could be used to control the risks and ultimately assist PHR providers in selecting a secure CSP for their customers' data. The section below gives more general guidelines that could assist CSPs to ensure they keep their customers' data secure.

4.4. General guidelines for CSPs

In addition to the proposed guidelines that can be used to mitigate the risk associated with cloud-based PHRs, this subsection provides additional general guidelines that were identified in the literature; and which could also guide CSPs to offer more secure products and services to their customers:

- **Identity and Access Management:** This aspect focuses on Authorisation, Authentication and Auditing (AAA). It ensures that only authorised parties can gain access to certain parts of the user's data (Kulkarni, Gambhir, Patil, & Dongare, 2012).
- **Compliance audits:** CSPs should adhere to the relevant laws and regulations that ensure compliance; and they should consent to audits that would serve to

verify and check that their policies are followed and are up-to-date (Beckers, Côté, Faßbender, Heisel, & Hofbauer, 2013).

- **Data protection laws and regulations:** Data in the cloud can be stored anywhere; therefore, it is difficult for users to know how their data are being protected. A solution could be for CSPs to develop products that are geographically limited; so as to restrict the location of the users' data (Svantesson & Clarke, 2010).
- **Compartmentalisation:** Data in the cloud are at risk of being compromised by other users; because the resources are shared amongst the different users. Compartmentalisation should be enforced, to ensure that customers may not access other customers' information (Mishra et al., 2011).
- **Data recovery:** Accidents, like computer crashes or hurricanes do happen; and it is therefore wise for the data in the cloud to be backed up and encrypted regularly (Subashini & Kavitha, 2011).
- **Backup and retention:** The Cloud Security Alliance proposes that users enter into a contractual agreement with their CSPs that would state the CSP's backup and retention strategies. They further advise that CSPs should implement strong key generation, storage and management, as well as destruction practices (Cloud Security Alliance, 2011).

This section has provided general guidelines in order to further advise CSPs on the steps to take to ensure that their data are private and secure.

4.5. Conclusion

This chapter has revisited the PHR dimensions mentioned in Chapter 2, together with the information-security risks identified in Chapter 3. The relationship between these entities was highlighted, in order to demonstrate how an information security risk factor can impact a PHR dimension, and thus the usability of a PHR. Guidelines that can be used to control these risks were formulated. The guidelines may help PHR providers to make an informed decision, when selecting a CSP to store the customers' data; and they should take into consideration the risks that were identified and assess whether the

CSP has taken the proposed steps to control them. General guidelines were also suggested for CSPs. These are security measures they can take, in addition to those which are already in the previous set of guidelines. This chapter's output helped in meeting the following sub-objectives

- Identify control measures, based on recognized best practices and frameworks, which can be used to mitigate the identified risks;
- Formulate guidelines that would assist PHR providers in choosing a secure CSP.

The next chapter provides information on how the research study was validated, i.e. the use of elite interviews and also presents the validated guidelines based on the results of the validation process.

Chapter 05: Validation of guidelines for secure cloud-based Personal Health Records

Chapter Content

CHAPTER 05: VALIDATION OF GUIDELINES FOR SECURE CLOUD-BASED PERSONAL HEALTH RECORDS

5.1. Introduction

Chapter Four proposed and discussed the preliminary guidelines for secure cloud-based Personal Health Records (PHRs). "Qualitative research aims to address questions concerned with developing an understanding of the meaning and experience dimensions of humans' lives and social worlds" (Fossey, Harvey, Mcdermott, & Davidson, 2015, p.716). As mentioned in Chapter One, this research study is of a qualitative nature; and therefore, in order to adequately address the research problem statement, a validation of the output (guidelines) had to be done. According to Eisner and Peshkin in (Cho & Trent, 2009), validity in qualitative research involves determining the extent to which the researcher's constructs of the knowledge correspond with the reality being studied. For this study, validation was tested through the use of elite interviews.

This chapter will describe the process that was followed to validate these guidelines *via* feedback gathered from the elite interviews that were conducted, as mentioned in Chapter One. The discussion will start by discussing the validation approach that was followed; the details of the elite interview process; the changes that have been implemented, based on the elite interview responses; and finally, the conclusion of the chapter. The final guidelines for secure cloud-based PHRs are presented in this chapter.

5.2. The elite interviews

As mentioned in Chapter One, the elites are those people who are considered superior, influential and/or well-informed in terms of ability or qualities compared with the rest of an organization or community (Elite, 2016; Marshall & Rossman, 2011).

Elites were identified, according to the different fields that relate to the study at hand, i.e. cloud computing, information security and health informatics (specifically PHRs) to take part in an elite interview. Elite interviews are used in order to validate what has been established from other sources, to ascertain what a set of people think, to interpret decisions gathered from a larger population, or to reconstruct an event or set of events (Tansey, 2007).The elites needed to have experience in one or more of these fields. The design of the elite interview data collection instruments will be described in the section that follows.

5.2.1. Design of the elite interview data collection instruments

This section discusses how the background documents and questionnaires were formulated that were used for data collection purposes during the validation process. The validation process was divided into 2 parts:

- Part 1 involved the validation of the classification of information security risks that could potentially impact PHR dimensions, as presented in Section 4.2, Chapter 4.
- Part 2 involved the validation of the preliminary guidelines for secure cloud-based PHRs, as presented in Section 4.3, Chapter 4.

For the two-part validation process, the participants in the elite interview were presented with a background document containing the relevant information required to prepare them for the validation process, as well as a questionnaire that was employed to obtain the validation data. The background document and the questionnaire were distributed to the elite interviewees via E-mail; and they were asked to return the completed questionnaires via E-mail as well.

For Part 1, which involved the validation of the classification of information security risks that may potentially impact PHR dimensions, the background document (Appendix C1) included an introductory section, where the background of the study was given. The PHR dimensions were explained in detail, in order to provide enough information for the classification. The different information security risks that might affect the given PHR dimensions were provided in a separate section. Here, the classification of the risks, according to the PHR dimensions was explained, as well as the exclusion of some of the PHR dimensions. The information security risks were then presented, together with the explanation of the PHR dimensions that the researchers classified under each risk. This background document provided insight that would then assist the elite when filling in the questionnaire (see Appendix C2) to validate the classification.

The background document prepared for Part 2 of the validation process (see Appendix D1) was related to the validation of the guidelines for secure cloud-based PHRs. The background of the study was provided in the first section of the document; and the problem description, the problem statement and the main objective of the research were also given. The second section provided the guidelines for secure cloud-based PHRs, giving a background on the different sources used, from which the guidelines were drawn, and also how each guideline addressed the information security risks. A separate questionnaire (see Appendix D2) was formulated, for the purpose of validating the guidelines.

Both questionnaires consisted of various sections, which covered the reviewer demographics, the quality, the utility and the efficacy of the classification of the information security risks impacting the PHR dimensions/ guidelines for secure cloud-based PHRs, as well as the overall impression of the background document. The evaluation of quality, utility and efficacy are in line with recommendations from Hevner, March, Park, and Ram (in (Venable, 2010). The authors state that utility is based on the usefulness, simplicity, understanding and practical usage of an artifact. Quality is based on evaluating whether the artifact is presented in a satisfactory manner. Finally, efficacy focuses on determining whether the artifact adopted will meet the required standard. Since the classification of the risks, according to PHR dimensions does not form an inherent part of the presentation of the final guidelines that will be utilized by PHR providers, it was not crucial to address utility. Quality and efficacy were therefore the only two evaluation criteria used for Part 1. Part 2 evaluated all three criterions.

Elites that were deemed knowledgeable in the required fields were identified. For the part 1 validation one elite was involved, which is referred to as elite 1A. For the part 2 validation there were two elites involved, referred to as elite 2A and 2B respectively. Responses to the respective questionnaires will be discussed separately in sections that follow.

5.2.2. Part 1 results

The subsections that follow will provide elite 1A's responses to the different sections of the questionnaire.

5.2.2.1. Demographics

The focus for this part of the validation process comprised identifying the elites with knowledge of PHRs, and also of information security. Elite 1A was identified as such an individual. Elite 1A is a Deputy Director in the ICT service delivery sector. His area of expertise is Information Technology. He has three years' experience in the field of health informatics (specifically PHRs); and he indicated that his level of knowledge, according to a Likert scale, is knowledgeable (3). The elites were asked to rate their level of knowledge as: (1) Not at all knowledgeable; (2) aware, but do not know much about; (3) knowledgeable; and (4) very knowledgeable. He has 17 years' experience in the field of information security; and he rated his level of knowledge in this field as very knowledgeable (4). Elite 1A further highlighted that he had completed a Master's degree in Information Technology, focusing on PHRs. The completed questionnaire can be viewed in Appendix C3.

This subsection has highlighted the demographical information on elite 1A. The next two subsections will report on his responses to the questions.

5.2.2.2. Quality of the classification of information security risk factors impacting PHR dimensions

This section of the questionnaire addressed the classification of information security risk factors and the PHR dimensions that each might impact. The elite was asked questions to determine whether he agrees with the classification. For the classification of each risk, he was given the option to indicate his level of agreement as: The elite's responses ranged from somewhat agree (3) to strongly agree (5). Because all of his responses indicated general agreement with the classification, no changes were made to the classification of risk factors impacting PHR dimensions.

5.2.2.3. Efficacy of the classification of information security risk factors impacting PHR dimensions

The elite was asked: "**In your opinion, do you think this classification of information security risk factors that might potentially impact PHR dimensions is adequate? Would you link the risk factors and the dimensions differently?"** and his response is given below with the action that was taken.

The elite's response:

"I am very impressed with the classifications of the PHR dimensions and the omission of the 3 dimensions not effected by information security risk factors. The alignment of risk factors to PHR dimensions is easily understandable and I am in agreement."

Action:

The elite's response was to agree with the omission of the 3 PHR dimensions, which validated the researcher's motivation to omit these dimensions (see section 4.2 In Chapter 4). His response further indicated that the classification of risk factors impacting PHR dimensions was adequate; and so, no further action is required in this regard.

5.2.2.4. Overall impression

The elite was asked to: "**Please provide any final comments, criticism or suggestions."** And his response is given next with the action that was taken.

The elite's response:

"A good piece of work. Perhaps look into the POPI act and how the requirements of this act will impact on information security pertaining to PHR's."

Action:

The POPI action is outside the scope of this research; because it focuses on the legislation involved in the security of PHRs; and it also focuses on South Africa. This is highlighted in the Delineation section of the dissertation (Chapter 1, section 1.5). The elite's response was therefore noted; but no action was taken.

The following section will describe part 2 of the validation process.

5.2.3. Part 2 results

The subsections that follow will provide elite 2A's and 2B's responses to the different sections of the questionnaire.

5.2.3.1. Demographics

For this part of the validation process, elites with knowledge of health informatics, information security and cloud computing were required. The two elites discussed next met these requirements.

Elite 2A is a director of a School of Information and Communication Technology (ICT) at a South African university. Her areas of expertise are health informatics and information security management. Elite 2A has 5 years' experience in the field of cloud computing and she rated her level of knowledge in this field as Knowledgeable (3). Elites were again asked to rate their level of knowledge as: (1) Not at all knowledgeable, (2) Aware but do not know much about, (3) Knowledgeable, and (4) Very knowledgeable. She has 11 years' experience in the field of health informatics (specifically PHRs) and her level of knowledge in this field was rated as Very knowledgeable (4). She also indicated that she has 20 years' experience in the field of information security with her level of knowledge in this field rated as Very knowledgeable (4).

Elite 2B is a Researcher at a leading South African research organization. His areas of expertise are cloud computing, information security and health informatics. He indicated that he has 5 years' experience in the field of cloud computing and that his level of knowledge is Very knowledgeable (4). The elite indicated that he has 5 years' experience in the field of health informatics and that his level of knowledge is Knowledgeable (3). He further indicated that he has 5 years' experience in the field of information security and that his level of knowledge in this field is Very knowledgeable (4). The completed questionnaire can be viewed on Appendix D3.

This section highlighted the demographical information on the two elites. The next sections will report on their responses to the questions.

5.2.3.2. Utility of the guidelines

This section of the questionnaire addressed the usability of the guidelines; and the elites were given open-ended questions to respond to. Table 5.1 provides the questions, the responses, and the actions taken to address them – where applicable.

Table 5.1: Elites' responses in terms of utility and actions taken to address them

Question	Elites' response	Action
1. Was the information provided in the document sufficient for a clear understanding of the need and function of the proposed guidelines?	**Elite 2A:** *"Section 1, which provides this information, was entirely clear."*	No action required.
	Elite 2B: *"The document is somehow sufficient with the exception of "Physical Intrusion". The PHR providers who are consumers of PaaS have limited control over the physical location of their hosted services. This guideline would be more relevant to IaaS providers and IaaS consumers. Instead, PHR providers may need to ensure that this is taken care of in the SLA."*	The comment is mostly addressing the quality part of the questionnaire, which will be reported on in the following section. How this was addressed will be answered there.
2. Was the description of the guidelines and control measures proposed to address the risks associated with cloud-based PHRs clear and easily understood?	**Elite 2A:** *"(1). The introductory part of Section 2 was very clear, except with regard to the "risk factors". I could not, from that section, deduce how the risk factors were identified. I later realised that the "Source" column in Table 2 indicated the source of the risk factors. Consider making clear in the introductory section that the risk factors were identified from literature which is specified in the "Source" column of Table 2. (2). The guidelines and control measures are clear as contained in Table 2. (3). There are some things in the detail description of the guidelines which are pointed out in questions 3.1 – 3.10 further below (where relevant)."*	As Elite 2A pointed out the process followed to identify the risks were not described in the background document provided to elites. In this dissertation the process is described in Chapter 1, Section 1.6.3 and is reiterated in section 5.4 where the final guidelines are presented.

Continuation of Table 5.1

Question	Elites' response	Action
	Elite 2B: *"Yes they are clear with the exception of Multi-tenancy. Separation of development, test and production facilities has nothing to do with multi-tenancy. Multi-tenancy can still be an issue in production facilities if there implementation flaws. A different solution may be required.*"	This response is in-line with only the first two controls presented for Multi-tenancy. Separation of tenants is a control given in the ISO standard therefore this solution was deemed sufficient for this risk. .
3. Can these guidelines be easily understood and utilized by PHR providers to make an informed choice when selecting a cloud service provider to ensure that their customers' data is kept private and secure?	**Elite 2A:** *"The guidelines are structured according to the risk factors that were identified from literature. Thus the structure is centred around the WHY "of the guidelines". I think it would help the PHR providers if the guidelines are structured according to the WHAT "of the guidelines". Thus rather than providing the guidelines per risk factor, you could make change the headings to be the guideline headings (or guideline topic) and within that explain which risk factor or factors are addressed by the guideline. It would also be useful if the bullet points could be presented more structured. For example, identify topics within each guideline. Present the requirements for the guideline in a table. First column topic (sub-topic of guideline); second column description; last column relevant standard. You should keep the $, * and # that you used in Table 2, within the description of the guidelines. Lastly, although the guidelines are for the PHR providers, there are also things mentioned which the CSP must do ("the CSP should provide"). This is understandable as you want the PHR provider to know that they should check for this. Suggestion: Split the guidelines discussion within each topic between "what the PHR provider should do" and "what the CSP should do". These suggestions are simply to assist with a clear presentation of the guidelines which may help the PHR providers to more easily understand and use the guidelines*"	The elite's responses were addressed in section 5.4, where the final guidelines are presented.

Continuation of Table 5.1

Question	Elites' response	Action
	Elite 2B: *"Yes they can be understood and utilized with the exception of physical intrusion and multi-tenancy as commented above."*	No action required.
4. Do you think these guidelines will be useful/ beneficial to PHR providers? Please elaborate on your answer.	**Elite 2A:** *"I definitely think that creating these guidelines will be both useful and beneficial to PHR providers because the information security controls that are required to address the risks are described in various standards, of which the PHR providers may not have the necessary expertise. The environment is complex in terms of both the risks and the possible controls thus these guidelines serve a useful purpose."*	No action required.
	Elite 2B: *"They will be very useful and beneficial. However, the guidelines may still be improved by considering threats that are more current such as the "The Treacherous 12 - CSA's Cloud Computing Top Threats in 2016" and "An analysis of security issues for cloud computing" by Hashizume et al (2013). The threats considered here were published some 4-5 years back. If guidelines of more recently published threats like the example above, it would be more beneficial."*	The sources mentioned by the elite were consulted and this led to the amendment of the risks, as seen in section 5.3. It was found that the risks mentioned in these sources are risks that are already addressed in the dissertation, just termed differently, and in some parts, categorized differently. There is only one risk from the Cloud Security Alliance document (2016) that was not addressed here. The risk on "Insecure Interfaces and APIs". This risk does not directly impact information security; so it is beyond the scope of this study. The risk descriptions have been amended to refer to the 2 sources, where appropriate.

5.2.3.3. Quality of the guidelines

These questions were presented in such a way that the elites were given a Likert scale to rate their level of agreement. Level 1 being strongly disagree and level 5 strongly agree. Most of the questions were answered with Agree by both elites. Where there was a response of Disagree and further comments given, responses will be presented in Table 5.2 below with the respective actions taken, where applicable.

Table 5.2: Elites' responses in terms of quality and actions taken to address them

Question	Elites' response	Action
1. **(a) Do you agree that the threat of "Malicious Insiders" can be mitigated by the guideline "Control access to PHR data"?** and **(b) Do you agree that the threat of "Malicious Insiders" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.1 in the background document?**	**Elite 2A Disagreed to both questions:** (a)*"I found the description of the risk factor / threat at the start of section 2.1 very confusing – specifically the reference to the CSP. I see the malicious insider in the context of this guideline, as someone who is working for the PHR provider, yet the description of the threat refers to the hiring practices of the CSP."* (b) *"It may be useful to include a reactive control / mechanism which allows audit logging and analysis to help uncover possible transgressions of employees/insiders (using their valid access rights)."*	Section 2.1 in the background document states that it is the CSP that is being referred to so no action was taken. A control for audit logging has been incorporated in the final guidelines (section 4.3.1).
2. **Do you agree that the threat of "Multi-tenancy" can be mitigated by the guideline "Separate customer data"?** and "**(b) Do you agree that the threat of "Multi-tenancy" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.3 in the background document?**	**Elite 2B Disagreed to both questions:** (a) *"See my comments on multi-tenancy above."* (b) "*Multi-tenancy as a property of the cloud is not an issue but threats associated with it are. Measures that address such threats are more desirable than taking away multi-tenancy. Having dedicated resources should be more expensive hence taking away the cost benefit."*	Threats associated with multi-tenancy have been presented in section 5.3.3
3. "**(a) Do you agree that the threat of "Data lock-in" can be mitigated by the guideline "Enforce technical interoperability"?** and "**(b) Do you agree that the threat of "Data lock-in" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.9 in the background document?**	**Elite 2A Disagreed to both questions:** (b) *"Enforcing technical interoperability but using only one CSP might not sufficiently mitigate the threat. You may need to supplement this with guidance around using a hybrid cloud approach."*	Action: As an addition to the guidelines, advice is given to the PHR provider to look into hybrid clouds as an alternate solution to this risk.

Continuation of Table 5.2

4. Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by the guideline "Report security incidents?" and "**Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.10 in the background document?**	**Elite 2A Disagreed to both questions:** (a) *"Reporting alone as a reactive measure is not enough to mitigate for DoS / DDoS / Botnets"* (b) *"There are definitely technical controls (proactive in nature) which the CSP will have to put in place to try and stop these kinds of attacks."* (b) "	Action: ISO 27017(2015) and the Cloud Security Alliance (2016) state that these type of incidents can only be "responded to". These attacks must first be visible, and then they will be acted upon (Cloud Security Alliance, 2016). Controls have been added in the final version of the guidelines (section 4.3.10).

5.2.3.4. Efficacy of the guidelines

This section of the questionnaire addressed the efficacy of the guidelines and the elites were given open-ended questions to respond to. Table 5.3 provides the questions, the responses, and the actions taken to address them – where applicable.

Table 5.3: Elites' responses in terms of efficacy and actions taken to address them

Question	Elites' response	Action
1. In your opinion, are the guidelines adequate to assist PHR providers in making an informed choice when selecting a cloud service provider to ensure that their customers' data remains private and secure? Or are there other relevant aspects that need to be considered?	**Elite 2A:** *"Indeed the guidelines will assist PHR providers to make an informed choice when selecting a CSP (based on security aspects). I do, however feel that the guidelines go beyond this and also address the PHR providers' responsibilities in terms of what security should be in place. Perhaps there is an argument that some of these responsibilities can be performed by either the PHR provider or the CSP. The way the guidelines were presented, however, implies "what all" should be done to mitigate the risks and does not necessarily say "your CSP should have the following in place in order for you to feel comfortable selecting them"*	The guidelines have been presented in such a way that it is clear who they are referring to (CSP versus PHR provider).
	Elite 2B: *"The guidelines are adequate. They can however still be improved by considering more recent threats in the cloud as published by the CSA."*	Comment already addressed as stated previously.
2. Do you think the use of these guidelines by PHR providers will contribute towards more secure cloud-based PHRs	**Elite 2A:** *"Certainly all controls that are put in place (because PHR providers are implementing the guidelines), will contribute to more secure cloud-based PHRs."*	No action required.

Continuation of Table 5.3

	Elite 2B: *"yes, definitely."*	No action required.
3. Do you agree that the different ISO standards used are adequate for the formation of the guidelines?	**Elite 2A:** *"I felt that the ISO27002 could be used to supplement / provide more information about the HOW – see also point 5.3 below. Alternatively it should be made clear that the scope is the WHAT and further details of the HOW can be found in the ISO27002."*	The scope of this research focuses on what should be done and not how it should be done because focusing on how it should be done addresses the CSPs and this research aims at addressing PHR providers.
	Elite 2B: *"Yes they are adequate and current."*	No action required.

5.2.3.5. Overall impression

This section of the questionnaire addressed questions on the overall impression of the guidelines; and the elites were given open-ended questions to respond to. Table 5.4 provides the questions, the responses, and the actions taken to address them – where applicable.

Table 5.4: Elites' responses in terms of overall impression and actions taken to address them

Question	Elites' response	Action
1. What is your overall opinion of the guidelines?	**Elite 2A:** *"The guidelines provide a useful reference for PHR providers in terms of consolidating the controls / measures that are required to secure cloud-based PHRs."*	No action required.
	Elite 2B: *"These guidelines are indeed a great initiative."*	No action required.
2. Can you recommend any way in which the guidelines can be improved?	**Elite 2A:** *Some comments were provided earlier about possibly structuring the guidelines differently to improve usability. In addition, I think you can check that the controls from the different standards are collated where relevant. For example, section 2.4 presents two actions (bullets) based on two standards. These essentially address the same thing thus could be one statement / action referencing both standards. This was also mentioned in section 3.3 (b). Also check this for all the other guidelines."*	The comment has been addressed in relevant sections under section 5.4.

Continuation of Table 5.4

	Elite 2B: *"As stated in earlier comments, it can still be improved by considering more recent threats as published by the CSA. Threats considered in the current guidelines were mostly published in 2011-2012 when the cloud was still in its early stages and some are indeed still prevalent to this day."*	Comments addressed in previous sections.
3. Please provide any final comments, criticism or suggestions.	**Elite 2A:** *"The guidelines focus a lot on WHAT and not HOW. Indeed, the scope of this project may have been on the WHAT and not the HOW. However, consider that the ISO27002 (according to which the ISO27799 is structured), does provide a lot of the HOW detail and thus your PHR provider should also be applying the guidance provided within the ISO27002. Refer to 10.4.1 in ISO27002 (related to 7.7.4.1 in ISO27799) as an example. This (ISO27002) would be applicable to all the guidelines from ISO27799."*	As the elite states, ISO 27799 is structured according to ISO 27002 and therefore the controls taken from the ISO 27799 were preferred for this research study as this standard is specifically addressing the security of personal health information.
	Elite 2B: *"Most of my criticism and suggestions are as stated in the earlier sections of this questionnaire. But mainly, it is the physical intrusion and multi-tenancy that need to be reconsidered. And lastly, to also consider more current literature on threats in the cloud."*	Responses have been addressed in previous sections.

After all the elites' responses had been analyzed, it was discovered that there may have been some confusion, which led to a possible limitation in terms of how they responded to some of the questions. These will be discussed in the following section.

5.2.4. Limitations of the elite interviews

The responses of the elites were partly influenced by some limitations and these are discussed below. Only part 2 of the validation process was influenced by these limitations:

The only notable limitation was seen with regard to how the elites interpreted the guidelines, as presented in the background document provided. There was confusion in terms of who the guidelines are aimed at, as stated by elite 2A. This is because of how the guidelines are written. Some of the responses, therefore, show that the elites were operating under the premise that the guidelines are directed at CSPs, and some at PHR providers. This has now been addressed by highlighting in section 5.4 to show that the guidelines are there to assist the PHR provider in making sure that they choose a CSP that adheres to the technical aspects addressed in the guidelines.

The sections that follow demonstrate how the elites' responses were incorporated into the revised identification of information security risks and the final guidelines for secure cloud-based PHRs.

5.3. Final information security risks relating to cloud-based Personal Health Records

This section presents the revised information security risks with regard to the suggestions made by elite 2B, as previously stated. Refer to Chapter 4, section 4.2, for the original risk descriptions.

5.3.1. Malicious insiders

When a PHR provider uses the cloud to store health data, he/she transfers trust to the provider of the cloud storage service. The CSP's staff members then have access to the PHR data and they may misuse their access rights to perform malicious attacks on the PHR users' data (Behl, 2011). "A malicious insider can have increasing levels of access to more critical systems and eventually to data" (Cloud Security Alliance, 2016, p.20). This leads to data leakage, as presented in (Cloud Security Alliance, 2016; Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013); where, a data leakage is said to happen when the data get into the wrong hands, while being transferred, stored, audited or processed. Malicious insiders can be categorised into the following groups:

- **Rogue administrator:** This type of insider could be an administrator employed by the CSP to back up and maintain their customers' data (Mahajan & Sharma, 2015). The rogue administrator could then use this access to hurt the CSP or the customers (Claycomb & Nicoll, 2012). This category of malicious insider can also be referred to as a third-party, which will be mentioned further down in the document.
- **Disgruntled employee:** This attacker targets his own employer, in other words the CSP. They use the cloud as a tool to carry out attacks on systems or data stored by the CSP (Claycomb & Nicoll, 2012; Mahajan & Sharma, 2015). This category of insider threat can also be present in the form of an employee, who was fired but still has active access rights to the system (Shiels & Valley, 2009).
- **Unintentional malicious insider:** An insider may be tricked by an outsider from a different organisation into performing an attack on the system of the former's employer. It is in fact a sabotage attack to expose the company's sensitive or embarrassing information (Claycomb & Nicoll, 2012).

5.3.2. Third-party access

The cloud-based PHR provider may also transfer some duties, such as the administration of the data, to a third party, which then creates a bigger pool of people who have access to the PHR data. The PHR user has no control over who sees his data, and what they do therewith, hence, the increasing the fear of unauthorised access to the user's PHR (Modi et al., 2013; Zissis & Lekkas, 2012).

5.3.3. Multi-tenancy

In cloud computing, users share resources, such as the Central Processing Unit (CPU), memory, networking capabilities, etc. (Cloud Security Alliance, 2016). This grants them direct access to the resources used by other users; because they use the same host machine. This poses the threat of attackers acting as PHR users, in order to gain access to other users' PHRs (Mishra et al., 2011). The identified risks that arise from multi-tenancy are:

- **System vulnerabilities:** Systems from different organizations are placed in close range to each other in the cloud computing environment; and because of multi-tenancy, this creates a new attack surface (Cloud Security Alliance, 2016).
- **Data scavenging:** Since tenants use the same resources in the cloud, the data that were deleted from one tenant may not be completely removed; so an attacker may be able to recover these data (Hashizume et al., 2013).

5.3.4. Software intrusions

A user's PHR data may be compromised through an injection of malicious software, e.g. a virus, which the attacker may then use to gain sensitive information, such as the log-in credentials of the user. Exploitable bugs are injected into programs, in order for the attackers to infiltrate a computer system for the purpose of stealing data, taking control of the system of disrupting service operations (Cloud Security Alliance, 2016). Some of the prominent risks associated with software intrusions are:

- **Account or service hijacking:** This is not a new threat; but cloud computing amplifies it. Phishing may also be used to this end (Wei et al., 2013). When an attacker gains access to one's credentials via phishing, or fraud, they can eavesdrop on the activities done on that particular system; and the system may become a new base for attackers (Cloud Security Alliance, 2016). The attacker may gain access to sensitive data, manipulate the data and redirect any transaction that is being performed (Hashizume et al., 2013).

- **Customer-data manipulation:** Web applications of users may be attacked by manipulating the data sent from their application component to the server's application (Hashizume et al., 2013).
- **Advanced Persistent Threats (APTs):** These are parasitical cyber-attacks that invade systems; in order to create a foothold in the computing environment of the companies they target, in order to smuggle data and intellectual property from a competitor (Cloud Security Alliance, 2016).

5.3.5. Physical intrusion

Cloud computing uses data centres to store the users' data. These are at a risk of being attacked physically; and such an attack may lead to hardware theft and/or unauthorised access to servers. Intruders may also have the intention of destroying the information via an information destruction attack (Hutchings et al., 2013).

5.3.6. Poor encryption key management

Users may be allowed to create their own decryption keys, and distribute them, as they see fit. If the keys fall into the wrong hands, the user's PHR data may be at risk. There is also a chance of password cracking, to which the PHR data may be vulnerable; if the encryption key management techniques are not of a good standard (AbuKhousa et al., 2012; Kuo, 2011). The lack of ongoing automated rotation of cryptographic keys, passwords and certificates, could lead to data breaches and enabling attacks (Cloud Security Alliance, 2016).

5.3.7. Temporary outages

Even though cloud computing is known for its high level of service reliability and availability; it can and does experience outages (AbuKhousa et al., 2012; W. Jansen & Grance, 2011). Cloud services experience outages, which may last for hours, preventing access to PHR data. Various risks may cause temporary outages; and these include risks that target the virtual machine (Hashizume et al., 2013).

5.3.8. Prolonged and permanent outages

A CSP may experience serious problems that may lead to bankruptcy or facility loss (W. Jansen & Grance, 2011). An accidental deletion or physical catastrophe may lead to the permanent loss of data (Cloud Security Alliance, 2016). This affects access to the users' PHRs for extended periods; and it sometimes even leads to the CSP's complete shutdown (W. A. Jansen, 2011).

5.3.9. Data lock-in

This is the inability of customers to move their data from one provider to the next, due to – for example – the current provider running out of business (Alex Mu-hsing Kuo, 2011). A PHR may need to be moved from one storage facility to another – for various reasons. Cloud computing makes this difficult; because most cloud infrastructures have little ability with respect to interoperability (W. A. Jansen, 2011).

5.3.10. Denial of Service (DoS)

This is performed by "saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner" (W. A. Jansen, 2011). This means that the attacker has leveraged cloud computing resources to perform various nefarious acts, which lead to the users not being able to access their applications and their data (Cloud Security Alliance, 2016). The attacker then prevents the PHR from processing any real requests from the user (Win et al., 2006).

The following section will present the final guidelines for secure cloud-based PHRs.

5.4 Final guidelines for secure cloud-based Personal Health Records

This section will present the final guidelines, based on revisions that were made to the guidelines presented in Chapter 4, section 4.3 after the elite interview validation process.

Table 5.5: Final guidelines for secure cloud-based PHRs

Guideline	Risk	Control Measures (ISO 27799:2008*, ISO 27017:2015 $ & ISO 17090-3:2008#)	Source
Control access to PHR data	Malicious insiders	• Access control policy (7.8.1.2)* • Access to networks and network services (9.1.2) $ • Roles and responsibilities; Screening; terms and conditions of employment (7.5.1)* • Management responsibilities: Information security awareness, education and training; Disciplinary process (7.5.2)* • Terminating responsibilities and return of assets; Removal of access rights (7.5.3)* • Audit logging (7.7.10.2) * • Protection of log information (7.7.10.4)* • User registration and deregistration (9.2.1) $ • Information access restriction (9.4.1) $	• Behl, 2011
Assess risks involved with third parties	Third-party access	• Assessment of risks related to external parties (7.3.3.1)* • Addressing security in third-party agreements (7.3.3.3)* • User access provisioning (9.2.2) $ • Management of privileged access rights (9.2.3) $ • Health information exchange policies, and procedures and exchange agreements (7.7.8.1)*	• Modi et al., 2013 • Sengupta, Kaulgud, & Sharma, 2011
Separate customer data	Multi-tenancy	• Separation of development, test and operational facilities (7.7.1.4)*, (12.1.4) $ • Segregation in networks (13.1.3) $	• Mishra et al., 2011 • Modi et al., 2013
Prevent malicious code infections	Software intrusion	• Controls against malicious code (7.7.4.1)* • Controls against malware (12.2.1) $	• Mahmood & Hill, 2011 • Wei et al., 2013
Store PHR data in secure data centres	Physical intrusion	• Physical security perimeter (7.6.1.1)*, (11.1.1) $ • Physical entry controls (11.1.2) $	• Hutchings et al., 2013
Adopt strong private key management techniques	Poor encryption key management	• Policy on use of cryptographic controls (10.1.1) $ • Key management (10.1.2) $ • Private key backup (7.6.2.5) # • Method of destroying private key (7.6.2.11) # • Avoid loss, disclosure or unauthorised use of private keys. If any occurs, report immediately (7.9.6.4) #	• AbuKhousa et al., 2012; • Alex Mu-hsing Kuo, 2011

Continuation of Table 5.5

Guideline	Risk	Control Measures (ISO 27799:2008*, ISO 27017:2015 $ & ISO 17090-3:2008#)	Source
Ensure business continuity	Temporary outages	• Security of network services (7.7.6.2)* • Alignment of security management for virtual and physical networks (CLD.13.1.4) $ • Administrator's operational security (CLD.12.1.5) $	• AbuKhousa et al., 2012 • Fernández-Cardeñosa, De La Torre-Díez, López-Coronado, & Rodrigues, 2012 • Onwubiko, Rimal, Choi, & Lumb, 2010
Backup and encrypt PHR data	Prolonged and permanent outages	• Health information backup (7.7.5)* • Information backup (12.3.1) $	• Jansen & Grance, 2011
Enforce technical interoperability	Data lock-in	• Compliance with security policies, standards and technical compliance (7.12.3)*	• Carroll et al., 2011 • Dillon, Wu, & Chang, 2010
Respond to information security incidents	Denial of Service (DoS)	• Reporting information security events and weaknesses (7.10.1)*, (16.1.2) $ • Responding to information security incidents (16.1.5) $	• AbuKhousa et al., 2012 • Carroll et al., 2011 • Modi et al., 2013

* denotes the use of the ISO 27799:2008 standard

$ denotes the use of the ISO 27017:2015 standard

# denotes the use of the ISO 17090:2008 standard

The sections that follow provide the identified guideline for each of the risks; and they explain what the PHR provider should look for when selecting a CSP.

5.4.1. Control access to PHR data

The **malicious insider** threat is very common in the cloud environment; and there is usually a lack of transparency on the hiring process of the CSP. There is no clarity on their hiring standards and practices; and this creates an opportunity for an opponent to gain access to sensitive information (Behl, 2011). The main guideline that has been identified to limit this risk is to **control access to PHR data**, which implies that the PHR provider should ensure that the CSP adheres to the following:

- In order to govern access to personal health information, an access control policy should be in place. It should be predefined, according to the roles with associated authorities, which are consistent, but limited to the needs of that particular role (7.8.1.2)*.
- Prior to employment, staff members should be given roles and responsibilities in the job description. A screening process should also be conducted to verify identity, living address, previous employment, as well as the terms and conditions of employment (7.5.1)*.
- During employment, staff members should be assigned responsibilities, offered information security awareness and training, and be informed of the disciplinary process (7.5.2)*.
- Upon termination or change of employment, access rights must be revoked (7.5.3)*.
- Systems that process personal health information should create a secure audit record every time a user accesses, creates, updates or archives personal health information via the system (7.7.10.2)*.
- Audit logs shall be secure and tamper-proof. The access to system audit tools and audit trails shall be secure to prevent misuse or compromise (7.7.10.4)*.

- The CSP should provide user registration and deregistration functions for the customers of the PHR provider. The specifications of how these functions work should also be provided to the PHR provider (9.2.1) [$].
- The CSP should provide access controls that allow PHR providers to restrict access to their cloud services, their cloud service functions and the PHR provider's data maintained in the service (9.4.1) [$].

The control below states what the PHR provider should do:

- The PHR provider's access control policy, which provides guidance on the use of network services, should specify the requirements for user access to each separate cloud service that is provided by the CSP (9.1.2) [$].

Implementing this guideline would ensure that the confidentiality of a PHR is preserved. Employees of the CSP would be governed by a control policy that would clearly state the role of each employee and the type of access he/she has. This would also protect the integrity of the data, because any employee who makes changes to the data without having the proper access rights would be held liable. Employees who are no longer with the CSP should have their access rights revoked; so as to prevent them from tampering with the availability, auditability and privacy of the PHR data.

5.4.2 Assess the risks involved with third parties

Adding more administrators to cloud systems increases the risk of unauthorised access (Modi et al., 2013). **Third parties** may pose a threat to the users of cloud services if they aim to use in a negative way the access that the CSP has granted them. Other risks involved with third parties include maintaining data confidentiality and integrity (Sengupta et al., 2011). The guideline that has been identified to limit this risk is to **assess the risks involved with third parties**, which implies that the PHR provider should ensure that the CSP adheres to the following:

- Conduct a risk assessment to weigh the risks that may be brought by third parties to the systems and the data. Security controls must subsequently be implemented, according to the identified level of risk and to the technologies used (7.3.3.1)*.

- When a third party is granted access to process personal health information, there must be formal contracts that specify the confidential nature and value of the personal health information; the security measures that must be implemented and complied with; limitations to access these services by third parties; and the penalty that would apply – should any of these security measures be breached (7.3.3.3)*.
- Support third-party identity and access management technologies for the cloud services and associated administration interfaces (9.2.2)[$].
- Provide sufficient authentication techniques for authenticating the PHR provider's administrators to the administrative capabilities of a cloud service, according to the identified risks (e.g. enable the use of third-party multi-factor authentication mechanisms) (9.2.3)[$].
- Information exchange agreements that specify the minimum set of controls to be implemented must also be formulated (7.7.8.1)*.

Third parties that have access to PHR data can be controlled in terms of the risks they could impose, should they perform malicious acts. The confidentiality, integrity, availability, auditability and privacy of PHRs can be maintained; if the risks that come with third parties are well-assessed and managed in time.

5.4.3 Separate customer data

The lack of compartmentalisation of resources in cloud computing allows users to access other users' personal information (Mishra et al., 2011). **Multi-tenancy** also makes it difficult to monitor and log the processes of virtual machines in the cloud (Modi et al., 2013). The guideline that has been identified to deal with this risk is to **separate customer data**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Development, testing and operational environments should be separated physically or virtually so as to reduce the risks of unauthorized access or changes to the operational environment (7.7.1.4)*, (12.1.4)[$].

In addition to this, the PHR provider should:

- Define its requirements for the segregation of networks in order to achieve tenant isolation in the shared environment of a cloud service, and to ensure that the CSP meets these requirements (13.1.3) $.

In order for PHRs to have confidentiality, integrity, availability and privacy, customer data should be separated.

5.4.4. Prevent malicious code infections

It is difficult to eliminate **software intrusions** in the cloud; and this raises concerns for prospective cloud customers. Malware also compromises the integrity of software in the cloud; because it can modify the victim's software somehow (Mahmood & Hill, 2011). The guideline that has been identified to deal with this risk is to **prevent malicious code infections**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Proper prevention, detection and response controls that are used to protect systems against malicious software must be adopted; and appropriate user awareness and training must be implemented (7.7.4.1)*.
- Detection, prevention and recovery controls to protect against malware should be implemented, in conjunction with the appropriate user awareness (12.2.1) $.

When PHRs are protected from software intrusions by preventing, detecting and properly responding to malicious code infections, the confidentiality, availability and privacy of PHRs would be preserved.

5.4.5. Store PHR data in secure data centres

The data centres that CSPs use to store the PHR data may be at risk of being attacked physically through the risk of **physical intrusion**, which would result in hardware theft, unauthorised access to servers, or the loss of access to data (Hutchings et al., 2013). The guideline that has been identified to limit this risk is to **store the PHR data in**

secure data centres. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Security perimeters should be defined and used to protect areas that contain information that is either sensitive or critical (11.1.1) [$]. There should be physical entry controls; offices should be secured; there should be protection against external and environmental threats; and public access, delivery and loading areas should be secure enough to prevent the loss of personal health information. These are all ways to prevent the public from getting too close to IT equipment. Software or equipment used to support a healthcare application that contains personal health information should not be removed from the site, or relocated within the organisation – without authorised permission from the organisation (7.6.1.1)*.
- Secure areas should be protected by appropriate entry controls, to ensure that only people with authorized access are allowed entry (11.1.2) [$].

The confidentiality, integrity, availability and privacy of PHRs would be protected if the data centres used to store PHR data are kept secure from external and environmental threats.

5.4.6. Adopt strong private key management techniques

Some systems allow users to generate their own decryption keys, and to distribute them to authorised parties (AbuKhousa et al., 2012). This may lead to **poor encryption key management;** since it becomes a challenge if the user loses the keys or discloses them to malicious parties (Kuo, 2011). For the purpose of the identified control measures, encryption keys are – from this point onwards – referred to as private keys; and the party responsible for keeping the keys is known as the certificate holder. The guideline that has been identified to deal with this risk is to **adopt strong private key management techniques**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Provide information to the PHR provider on the circumstances in which it uses cryptography to protect the information it processes. The CSP should also let the

PHR provider know whether it can offer them any capabilities that allow the PHR provider to perform its own cryptographic protection (10.1.1) [$].

- It is recommended that the certificate holder creates a backup of the private keys, where possible. This backup would be held in the environment of the certificate holder; and it would be entirely in his/her control (7.6.2.5) [#].
- When the private key is no longer in use, all its copies in computer memory and shared disk space must be securely destroyed by overwriting multiple times (7.6.2.11) [#].
- A certificate holder must ensure that he/she makes every effort to avoid the loss, disclosure or unauthorised use of the private keys. If there is any actual or suspected loss, disclosure or other compromise of the private key, the certificate holder must immediately notify the certification authority (7.9.6.4) [#].

In addition to the controls above, the PHR provider should:

- Not allow the CSP to store and manage the encryption keys for cryptographic operations, when it uses its own key management, or a separate distinct key management service (10.1.2) [$].

When encryption keys are managed and disposed of properly, the confidentiality, availability and privacy of PHR data can be ensured.

5.4.7. Ensure business continuity

It is vital that systems that process health information in the cloud should be available continuously without any interruptions (AbuKhousa et al., 2012). Outages are not exclusive to cloud environments; but they are highlighted there because of the interconnectedness of their services (Gonzalez et al., 2011). A **temporary outage** could be caused by a natural disaster, vulnerability exploits and deliberate attacks (Onwubiko et al., 2010). Health organisations recognise business continuity management as a requirement; and this includes disaster recovery (International Organization for Standardization, 2008). The guideline that has been identified to limit this risk is to **ensure business continuity**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Carefully consider what impact the loss of network service availability would have on clinical practice (7.7.6.2)*.
- In a cloud computing environment, the inconsistency of network policies can cause system outages. The CSP should define and document an information security policy for the physical network (CLD.13.1.4) [$].

In addition to the controls above, the PHR provider should:

- Create a document that contains procedures for critical operations, where failure can cause irreparable damage to assets in the cloud computing environment. This document should specify that a supervisor should monitor such operations (CLD.12.1.5) [$].

In case a PHR goes offline, or is unavailable for any reason, business continuity should be ensured by considering the impact that this would have, and taking measures to avoid such.

5.4.8. Backup and encrypt PHR data

When the cloud that is used for storage, experiences **prolonged and permanent outages**, it has a negative impact on the customer who relies on the data. It is important for a CSP to have a plan for how the data would be recovered; and to ensure that it is still accessible (W. Jansen & Grance, 2011). The guideline that has been identified to limit this risk is to **back up and encrypt PHR data**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- In order to make sure that personal health information would be available in the future; it should be backed up and stored in a physically secure environment (7.7.5)*.

In addition to the above control, the PHR provider should:

- Request the specifications of the backup capability in a case where the CSP provides backup capabilities as part of the cloud service (12.3.1) [$].

PHR data should be backed up and encrypted to ensure their availability.

5.4.9. Enforce technical interoperability

It is possible for customer data to experience **data lock-in** in the cloud – due to a number of reasons – such as the provider going out of business (Carroll et al., 2011). The lack of interoperability between cloud services prohibits customers from utilising multiple providers at the same time (Dillon et al., 2010). The guideline that has been identified to deal with this risk is to **enforce technical interoperability**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Systems that process personal health information need to be technically interoperable; since many of them typically consist of different interoperating systems (7.12.3)*.

In addition to the above control, the PHR provider should:

- Consider using the hybrid cloud approach. This is a private cloud that is linked to one or more external cloud services that are managed centrally and provisioned as a single unit (Ramgovind et al., 2010). This can be used to mitigate data lock-in where the public cloud can be used to capture the extra tasks that cannot be easily run in the data centre – due to temporary heavy workloads (Armbrust et al., 2010).

It is vital for PHRs to be interoperable with other health systems, in order for them to be deemed useful.

5.4.10. Respond to information security incidents

Denial of Service (DoS) poses numerous threats in the cloud computing environment (Carroll et al., 2011). By attacking one server, the attacker may affect the availability of other services as well (Modi et al., 2013). This threat is intensified in a health system that becomes unavailable, especially in an emergency situation (AbuKhousa et al., 2012). The guideline that has been identified to limit this risk is to **respond to information security incidents**. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Report security incidents. These include corruption or unintentional disclosure of personal health information, or the loss of availability of health information systems, where such a loss affects the patient's care in an undesirable manner (7.10.1)*. Have mechanisms in place that allow the PHR provider to report an information security event to the CSP. The CSP should also report any information security event to the PHR provider, and also keep track of the status of the reported information security event (16.1.2) $.

- Respond to information security incidents. This involves the collection of evidence as soon as possible after the incident has occurred; conducting information security forensic analysis; ensuring that all involved response activities are properly logged for later analysis; dealing with information security weaknesses that led to, or contributed to, the incident (16.1.5) $.

For PHRs to be kept available all the time, security incidents should be reported to the PHR providers; so that they can provide other means to keep the PHR accessible. Action also needs to be taken, in order to properly respond to and avoid the incident from recurring.

The above section has provided the guidelines that can be used to control the risks and ultimately assist PHR providers in selecting a secure CSP for their customers' data. The next section concludes this chapter.

5.5. Conclusion

This chapter has discussed the validation process followed for the output of this research study: i.e. guidelines for secure cloud-based PHRs. Elite interviews were followed as the validation approach; and this process was explained earlier in this chapter. The responses from the elites were also presented; and these led to the refinement of both the information security risks and the guidelines, as presented here. The next chapter concludes the study.

Chapter 6- Conclusion

Contents

CHAPTER 6: CONCLUSION

6.1. Introduction

Health is one of the most important factors that one has to manage, as a part of one's daily living. Using paper records to store and manage past and current illnesses has proven to be a challenge, when it comes to accessibility and storage. The introduction of PHRs is one way of simplifying health management. As discussed in Chapter 2, PHRs are personally managed by the individuals; and they decide who may have access to these records, e.g. their physicians, caregivers, etc.

PHRs can be stored locally on a web server or via cloud computing. As argued in Chapter 2, cloud computing introduces numerous benefits for the storage and processing of information. Storing PHRs in the cloud environment is beneficial for both the PHR owners and the PHR providers. PHR owners get extensive access to their health data, as long as there is an internet connection. They get to use the resources as needed, which promotes great scalability. PHR providers get to cut operational costs because they transfer all the IT infrastructure and maintenance costs to the CSP.

As much as cloud computing brings all these added benefits to PHRs, it comes with serious security concerns, which is what led to this research. Cloud computing involves many uncertainties that should be considered before any kind of business decides to migrate to the cloud.

The main problem addressed in this research is that: **There is a lack of guidance to assist PHR providers in making an informed choice when selecting a CSP, to ensure their customers' data are kept private and secure**.

The primary objective of the current research therefore, was **to propose guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure their customers' data remain private and secure.**

The following sections will provide a summary of the accomplishment of research objectives, the findings, research limitations, a summary of the contributions and some suggestions for further research.

In order to structure the research in hand, a problem statement was defined, objectives were set, and research methods were defined and applied by following an appropriate research process. The next section will show how the research objectives were accomplished.

6.2. Accomplishment of Research Objectives

This section will recapitulate the primary and secondary research objectives, explaining how and where in the study each was met.

6.2.1. Primary and secondary objectives

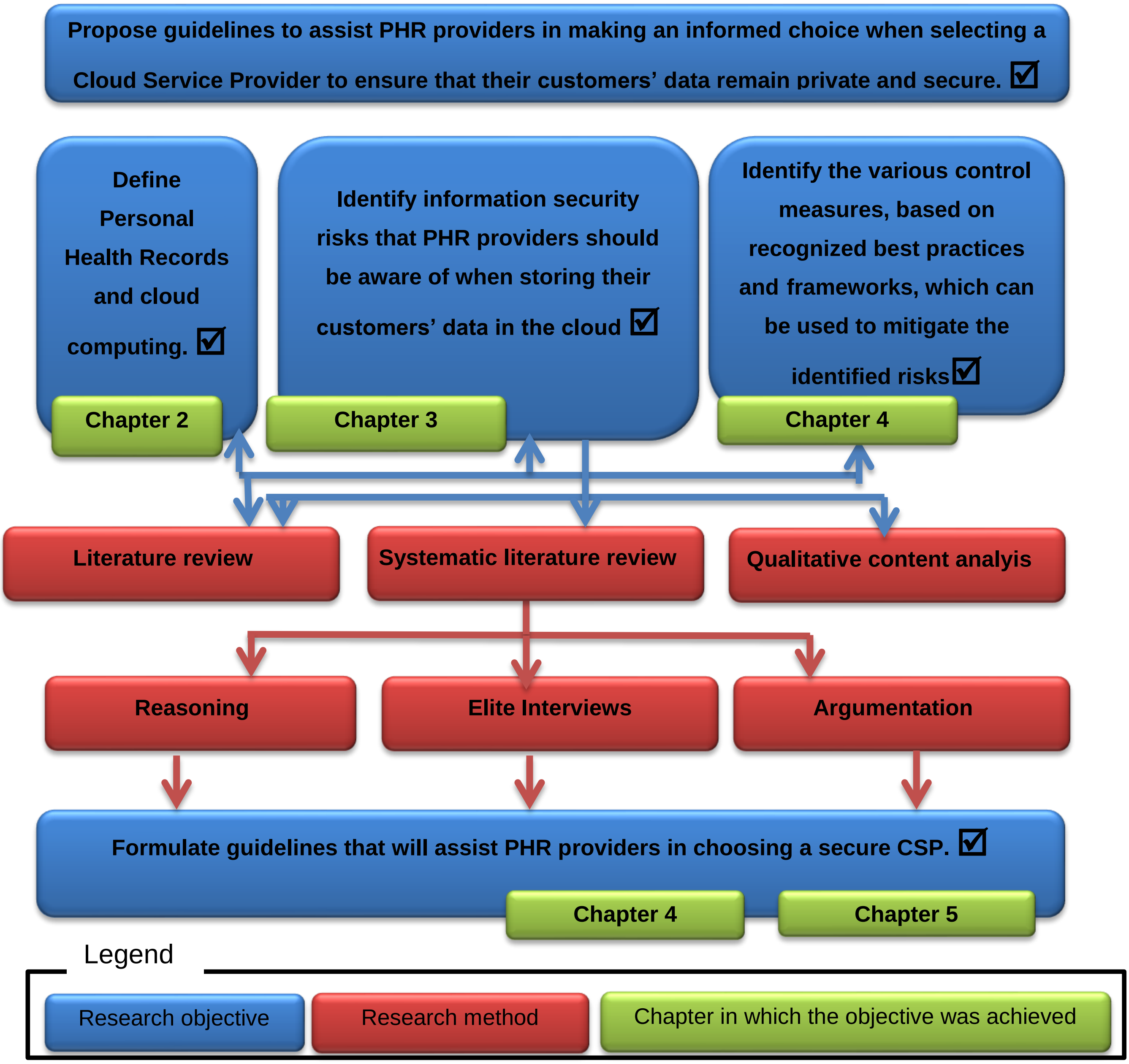
The primary objective of the research in hand is to propose guidelines to assist PHR providers in making an informed choice, when selecting a CSP to ensure that their customers' data remain private and secure. The primary objective is supported by the following secondary objectives:

- Define Personal Health Records and cloud computing.
- Identify information security risks that PHR providers should be aware of when storing their customers' data in the cloud.
- Identify the various control measures, based on recognised best practices and frameworks, which can be used to mitigate the identified risks.
- Formulate guidelines that would assist PHR providers in choosing a secure CSP.

The primary objective addresses the problem statement of this research. The secondary objectives collectively meet the primary objective. The subsection that follows illustrates how these objectives were met; and it also highlights where they were achieved in the study at hand.

The diagram below illustrates how the research process was followed, in terms of the already-mentioned objectives. It will highlight whether each objective was achieved or not; and it will also show where in the dissertation each objective was achieved. This will be followed by a brief discussion on each of the secondary objectives.

Figure 6.1: The research process



- **Define Personal Health Records and cloud computing**

Chapter 2 presented more details in respect of PHRs by focusing on the definitions, types of PHRs, benefits and also some barriers to adoption. The concept of cloud computing was discussed in greater detail here. It was clearly defined; and its features were highlighted; while service and deployment models, benefits and drawbacks were also discussed. This chapter addressed the first research objective, which was to define PHRs and cloud computing.

- **Identify information security risks that PHR providers should be aware of when storing their customers' data in the cloud.**

A systematic literature review and qualitative content analysis was conducted for the Chapter 3 content, in order to identify the information security risks that apply when using cloud computing services. The risks were divided into two categories, which helped to focus the research on information security. Hence, the second objective was addressed by this chapter.

- **Identify the various control measures, based on recognized best practices and frameworks, which can be used to mitigate the identified risks**

In Chapter 4, the risks were revisited, together with the PHR dimensions discussed in Chapter 2. This was done, so as to show the link between the two. The identified risks each had an impact on most of the dimensions, which affected the security and usability of a PHR. While the literature review was conducted, control measures that could be used to address each risk were also identified.

- **Formulate guidelines that would assist PHR providers in choosing a secure CSP.**

The security measures identified in the above sub-objective helped greatly in formulating the guidelines for limiting the risks associated with cloud computing. The relevant ISO standards were consulted; since this research focused on information security in health information. Controls were identified, according to the risks that they would mitigate; and this formed the basis of the guidelines. Chapters 4 and 5 thus addressed the last two objectives. Chapter 5 provided the validation of the guidelines via the use of elite interviews. The responses from the elites helped refine the information security risks and the guidelines for secure cloud-based PHRs.

The above section reiterated the objectives of this study, and highlighted that they were achieved successfully by showing the chapters that contain each. The following section will provide a summary of the findings.

6.3. Summary of the findings

The problem statement of this research stated that there is a lack of guidance to assist PHR providers in terms of aspects that they should consider when selecting a CSP to ensure that their customers' data are kept private and secure. The findings drawn from this are as follows:

- The usefulness of a PHR can be determined by looking at the particular dimensions that it has.
- PHRs offer great benefits for patients, caregivers and physicians; and they also have economy-related benefits.
- Even though there are such benefits, there are also adoption barriers for the use of PHRs; and these are mostly privacy and security concerns.
- PHRs can be stored by using cloud computing. This is a beneficial way of storing and accessing information on the internet; but it also comes with a lot of information security risks.
- The information security risks that affect PHRs when they are stored in the cloud largely affect the PHR dimensions as well.
- There are security measures that can be taken to mitigate these information security risks.
- Guidelines can be drawn from the relationship between the PHR dimensions and the information security risks that impact them, together with the identified security measures to mitigate these risks.

Information security risks that directly impact the PHR dimensions were identified and reported on in previous chapters. This was done in order to correctly identify the guidelines that directly mitigate each risk for the PHR dimensions to be adequately preserved. Table 6.1 represents the findings of this research study, i.e. the link between information-security risks, PHR dimensions and the formation of the guidelines.

Table 6.1: Information security risks, PHR dimensions and guidelines

Risk	**PHR Dimension Impacted by Risk**						**Guideline**	**Control Measures (ISO 27799:2008*, ISO 27017:2015 [$]& ISO 17090-3:2008[#])**	**Source**
	Confidentiality	**Integrity**	**Availability**	**Auditability**	**Privacy**	**Interoperability**			
Malicious insiders	✓	✓	✓	✓	✓		• Control access to PHR data	• Access control policy (7.8.1.2)* • Access to networks and network services (9.1.2) [$] • Roles and responsibilities; Screening; Terms and conditions of employment (7.5.1)* • Management responsibilities; Information security awareness, education and training; Disciplinary process (7.5.2)* • Terminating responsibilities and return of assets; Removal of access rights (7.5.3)* • User registration and deregistration (9.2.1) [$] • Information access restriction (9.4.1) [$]	• Behl, 2011
Third-party access	✓	✓	✓	✓	✓		• Assess risks involved with third parties	• Assessment of risks related to external parties (7.3.3.1)* • Addressing security in third-party agreements (7.3.3.3)* • User access provisioning (9.2.2) [$] • Management of privileged access rights (9.2.3) [$] • Health information exchange policies and procedures and exchange agreements (7.7.8.1)*	• Modi et al., 2013 • Sengupta, Kaulgud, & Sharma, 2011
Multi-tenancy	✓	✓	✓		✓		• Separate customer data	• Separation of development, test and operational facilities (7.7.1.4)*, (12.1.4) [$] • Segregation in networks (13.1.3) [$]	• Mishra et al., 2011 • Modi et al., 2013
Software intrusions	✓		✓		✓		• Prevent malicious code infections	• Controls against malicious code (7.7.4.1)* • Controls against malware (12.2.1) [$]	• Mahmood & Hill, 2011 • Wei et al., 2013

Continuation of Table 6.1

Risk	PHR Dimension Impacted by Risk: Confidentiality	Integrity	Availability	Auditability	Privacy	Interoperability	Guideline	Control Measures (ISO 27799:2008*, ISO 27017:2015 $& ISO 17090-3:2008#)	Source
Physical intrusions	✓	✓	✓		✓		• Store PHR data in secure data centres	• Physical security perimeter (7.6.1.1)*, (11.1.1) $ • Physical entry controls (11.1.2) $	• Hutchings et al., 2013
Poor encryption key management	✓		✓		✓		• Adopt strong private key management techniques	• Policy on use of cryptographic controls (10.1.1) $ • Key management (10.1.2) $ • Private key backup (7.6.2.5) # • Method of destroying private key (7.6.2.11) # • Avoid loss, disclosure or unauthorised use of private keys. If any occurs, report immediately (7.9.6.4) #	• AbuKhousa et al., 2012; • Alex Mu-hsing Kuo, 2011
Temporary outages			✓				• Ensure business continuity	• Information security aspects of business continuity management (disaster recovery) (7.11)* • Security of network services (7.7.6.2)* • Alignment of security management for virtual and physical networks (CLD.13.1.4) $ • Administrator's operational security (CLD.12.1.5) $	• AbuKhousa et al., 2012 • Fernández-Cardeñosa, De La Torre-Díez, López-Coronado, & Rodrigues, 2012 • Onwubiko, Rimal, Choi, & Lumb, 2010
Prolonged and permanent outages			✓				• Backup and encrypt PHR data	• Health information backup (7.7.5)* • Information backup (12.3.1) $	• Jansen & Grance, 2011
Data lock-in						✓	• Enforce technical interoperability	• Compliance with security policies, standards and technical compliance (7.12.3)*	• Carroll et al., 2011 • Dillon, Wu, & Chang, 2010
Denial of Service (DoS)			✓				• Respond to information security incidents	• Reporting information security events and weaknesses (7.10.1)*, (16.1.2)$ • Responding to information security incidents (16.1.5) $	• AbuKhousa et al., 2012 • Carroll et al., 2011 • Modi et al., 2013

* denotes the use of the ISO 27799:2008 standard
$ denotes the use of the ISO 27017:2015 standard
# denotes the use of the ISO 17090:2008 standard

This section has summarized the overall findings of this study, highlighting the major conclusions drawn from the previous chapters. The next section will report on the research limitations.

6.4. Research limitations

The guidelines presented in Chapter 5 are limited; because they are relevant only to PHR providers. Furthermore, PHR owners were not given any guidance on how to choose a cloud-based PHR provider – despite the fact that the risks that were identified were technical in nature, and avoiding them would require a certain level of expertise.

The guidelines focused exclusively on cloud-based storage of PHRs; and they did not consider any of the other types of PHRs that were identified in Chapter 2 of this dissertation.

Although the cloud computing risks identified in this research can affect any domain, and not only the healthcare sector; the present study, nevertheless, focused entirely on health information.

The identification of research limitations has created room for the formulation of future research goals, which will be discussed next.

6.5. Suggestions for future research

The guidelines should be extended to accommodate PHR owners. They need to know what to look for in a cloud-based PHR provider – before deciding to move their health records.

General guidelines should be developed for the proper storage of PHRs – and not only for PHRs that are stored in the cloud; because the internet as a whole has security issues that need to be taken into consideration.

Cloud computing is a domain that has given rise to many privacy and security issues. Any sensitive information stored in the cloud, therefore, needs to be protected. Generic guidelines that can ensure the security of any type of sensitive information stored in the cloud should be developed, taking into account the risks already identified in this research.

6.6. Summary

This chapter has concluded the research by revisiting and summarising the previous chapters and their content. The research objectives that were set at the beginning of this dissertation were met by using the specified research methods. The limitations of this research were also recognised; while possible future research that could stem from this dissertation was additionally indicated.

The emergence of cloud-based PHRs has brought along a number of benefits in the healthcare industry; and, as such, the providers of this service need proper guidance to make sure that their PHR data remain private and secure.

This research aimed at assisting a PHR provider in making sure that they select a CSP that adheres to the technical aspects addressed in the guidelines. The Cloud Security Alliance (CSA) (2016) states that insufficient due diligence in selecting a CSP is a security concern for cloud adoption. Providing these guidelines could, therefore, ensure that PHR providers perform due diligence. They can also aid in the better use of cloud facilities, as well as those of PHRs, by potentially diminishing some of the risks associated with offering cloud-based PHRs.

References

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Challenges. *Future Internet*, *4*(3), 621–645. http://doi.org/10.3390/fi4030621

Adhikari, R., Richards, D., & Scott, K. (2014). Security and Privacy Issues Related to the Use of Mobile Health Apps. *25th Australasian Conference on Information Systems (ACIS 2014)*, (Schulke 2013).

Akande, A. O., April, N. A., Van Belle, J.-P., Town, C., & Belle, J. Van. (2013). Management Issues with Cloud Computing. *ACM International Conference Proceeding Series*, 119–124. http://doi.org/10.1145/2556871.2556899

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. a, & Straus, S. E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 515–522. http://doi.org/10.1136/amiajnl-2011-000105

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A view of Cloud Computing. *Communications of the ACM*, *53*(4), 50–58.

Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *1*(2), 234–245.

Baliga, J., Ayre, R. W. a, Hinton, K., & Tucker, R. S. (2011). Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport. *Proceedings of the IEEE*, *99*(1), 149–167. http://doi.org/10.1109/JPROC.2010.2060451

Barnett, E. (2011). What is the difference between spam, malware and phishing? Retrieved February 18, 2015, from http://www.telegraph.co.uk/technology/8267578/What-is-the-difference-between-spam-malware-and-phishing.html

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013). *A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering* *security, privacy, and legal compliance*. *Requirements Engineering* (Vol. 18). http://doi.org/10.1007/s00766-013-0174-7

Bégin, M. ., Jones, B., Casey, J., Laure, E., Grey, F., Loomis, C., & Kubli, R. (2008). *AN EGEE COMPARATIVE STUDY : GRIDS AND CLOUDS - EVOLUTION OR REVOLUTION*.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. *Proceedings of the 2011 World Congress on Information and Communication Technologies, WICT 2011*, 217–222. http://doi.org/10.1109/WICT.2011.6141247

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches, *34*(January), 257–286.

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *InfoWorld*, *July*, 2–3. Retrieved from http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

Bryman, A. (2012). *Social research methods* (Fourth). Oxford University Press. Retrieved from https://books.google.co.za/books?id=vCq5m2hPkOMC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Carlson, T. (2001). Information Security Management : Understanding ISO 17799. *Lucent Technologies Worldwide Services*, (October), p.4,5,6,7,8.

Carrion, I., Fernandez Aleman, J., & Toval, A. (2012). Personal Health Records: New Means to Safely Handle our Health Data? *Computer*. http://doi.org/10.1109/MC.2012.74

Carroll, M., Van Der Merwe, A., & Kotzé, P. (2011). Secure Cloud Computing: Benefits, Risks and Controls. *Information Security for South Africa*, 1–9. http://doi.org/10.1109/ISSA.2011.6027519

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*, *1*(973), 647–651. http://doi.org/10.1109/ICCSEE.2012.193

Cho, J., & Trent, A. (2009). Qualitative Research.

http://doi.org/10.1177/1468794106065006

Choubey, R., Dubey, R., & Bhattacharjee, J. (2011). A survey on cloud computing security, challenges and threats. *International Journal on Computer …*, *3*(3), 1227–1231. Retrieved from http://www.doaj.org/doaj?func=fulltext&aId=719357

Claycomb, W. R., & Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. *Proceedings - International Computer Software and Applications Conference*, 387–394. http://doi.org/10.1109/COMPSAC.2012.113

Clinch, J. (2009). Itil v3 and information security. *White Paper*, (May), 1–40. Retrieved from http://www.best-management-practice.com/knowledge-centre/white-papers/

Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. *Cloud Security Alliance*, *3*, 155. http://doi.org/10.1016/S1353-4858(99)90042-9

Cloud Security Alliance. (2016). Cloud Computing Top Threats in 2016 The Treacherous 12, (February).

Creswell, J. W. (2013). *Research design: Qualitative, Quantitative and Mixed methods approaches*. *Journal of Chemical Information and Modeling* (Fourth, Vol. 53). London: SAGE Publications Inc. http://doi.org/10.1017/CBO9781107415324.004

Detmer, D. E., Bloomrosen, M., Raymond, B., & Tang, P. (2008). Integrated personal health records: Transformative tools for consumer-centric care. *BMC Medical Informatics and Decision Making*, *8*(1), 45. http://doi.org/10.1186/1472-6947-8-45

Dillon, T., Wu, C. W. C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 27–33. http://doi.org/10.1109/AINA.2010.187

Elite. (2016). Retrieved April 11, 2016, from http://www.oxforddictionaries.com/definition/english/elite

Elky, S. (2006). *An Introduction to Information System Risk Management*.

Elmogazy, H., & Bamasak, O. (2013). Towards healthcare data security in cloud computing. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 363–368. http://doi.org/10.1109/ICITST.2013.6750223

Endsley, S., Kibbe, D. C., Linares, A., & Colorafi, K. (2006). An introduction to personal health records. *Family Practice Management*, *13*(5), 57–62.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. http://doi.org/10.1016/j.jbi.2012.12.003

Fernández-Cardeñosa, G., De La Torre-Díez, I., López-Coronado, M., & Rodrigues, J. J. P. C. (2012). Analysis of cloud-based solutions on EHRs systems in different scenarios. *Journal of Medical Systems*, *36*(6), 3777–3782. http://doi.org/10.1007/s10916-012-9850-2

Forman, J., & Damschroder, L. (2007). Qualitative Content Analysis. In L. Jacobsy & L. Siminof (Eds.), *Emperical Methods for Bioethics: A primer*. Elsevier JAI.

Fossey, E., Harvey, C., Mcdermott, F., & Davidson, L. (2015). Understanding and evaluating qualitative research. http://doi.org/10.1046/j.1440-1614.2002.01100.x.Understanding

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud computing and grid computing 360-degree compared. *Grid Computing Environments Workshop 2008 (GCE '08)*, 1–10. http://doi.org/10.1109/GCE.2008.4738445

Fuji, K. T., Abbott, A. a., Galt, K. a., Drincic, A., Kraft, M., & Kasha, T. (2012). Standalone personal health records in the United States: meeting patient desires. *Health and Technology*, *2*(3), 197–205. http://doi.org/10.1007/s12553-012-0028-1

Geelan, J. (2009). Twenty-One experts define Cloud computing. Retrieved February 18, 2014, from http://www.vertualization.sys-con.com/node/612375?page=0,0

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, *8*(4), 597–607.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). The Characteristics of Cloud Computing. *2010 39th International Conference on Parallel Processing Workshops*, 275–279. http://doi.org/10.1109/ICPPW.2010.45

Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 231–238.

http://doi.org/10.1109/CloudCom.2011.39

Gordon, G. (2002). Dozens of threats beset your data. Retrieved April 23, 2015, from http://www.suntimes.co.za/2002/05/12/

Grossman, R. L. (2009). The case for cloud computing. *IT Professional*, *11*(2), 23–27. http://doi.org/10.1109/MITP.2009.40

Gunawi, H. S., Hao, M., Suminto, R. O., Laksono, A., Satria, A. D., Adityatama, J., & Eliazar, K. J. (2016). Why Does the Cloud Stop Computing? Lessons from Hundres of Service Outages. *Proceedings of the Seventh ACM Symposium on Cloud Computing - SoCC '16*, 1–16. http://doi.org/10.1145/2987550.2987583

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer Communications*, *22*, 885–897. http://doi.org/10.1016/S0140-3664(99)00064-X

Harvey, W. S. (2010). Methodological approaches for interviewing elites. *Geography Compass*, *4*(3), 193–205. http://doi.org/10.1111/j.1749-8198.2009.00313.x

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. http://doi.org/10.1186/1869-0238-4-5

Hutchings, A., Smith, R. G., & James, L. (2013). Cloud computing for small business: Criminal and security threats and prevention measures, (456).

Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing*, *14*(5), 14–22. http://doi.org/10.1109/MIC.2010.86

International Organization for Standardization. (2008). *Health informatics — Information security management in health using ISO/IEC 27002* (Vol. 2008). Switzeralnd.

International Organization for Standardization. (2009). *SANS 17090-3 : 2009 SOUTH AFRICAN NATIONAL STANDARD Health informatics — Public key infrastructure Part 3 : Policy management of certification authority*.

International Organization for Standardization. (2011). *SANS 27005 : 2012 (ISO/IEC 27005:2011) SOUTH AFRICAN NATIONAL STANDARD Information technology — Security techniques — Code of practice for information security management*.

ISACA. (2012). *COBIT 5 for Information Security*. USA.

ISACA. (2013). COBIT 5: Enabling I nformation.

Jansen, W. A. (2011). Cloud hooks: Security and privacy issues in cloud computing. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. http://doi.org/10.1109/HICSS.2011.103

Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *Director*, *144*(7). http://doi.org/10.3233/GOV-2011-0271

Kaelber, D., Jha, A., Johnston, D., Middleton, B., & Bates, D. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, *15*(6), 729–736. http://doi.org/10.1197/jamia.M2547.Introduction

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: an evaluation of features and functionality. *International Journal of Medical Informatics*, *81*(9), 579–93. http://doi.org/10.1016/j.ijmedinf.2012.04.007

Kim, M. I., & Johnson, K. B. (2002). Personal Health Records: Evaluation of Functionality and Utility. *Journal of the American Medical Informatics Association*, *9*(2), 171–180. Retrieved from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3128401&tool=pmcentrez&rendertype=abstract

Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2010). Ubiquitous access to cloud emergency medical services. In *… and Applications in …* (pp. 1–4). http://doi.org/10.1109/ITAB.2010.5687702

Krutz, R., & Vines, R. (2010). *Cloud Security: A comprehensive guide to secure cloud computing*. Wiley Publishing Inc. Retrieved from http://www.springerlink.com/index/J7X2571313853386.pdf

Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012). A security aspects in cloud computing. *2012 IEEE International Conference on Computer Science and Automation Engineering*, 547–550. http://doi.org/10.1109/ICSESS.2012.6269525

Kumar, K., Akash, D., Somesh, W., & Dewangan, K. (2013). A Valued Analysis of Information Security , Threats and Solutions for Cloud Computing, *2*(9), 648–658.

Kuo, A. M. (2011). Opportunities and challenges of cloud computing to improve health care services. *J Med Internet Res*, *13*(3), e67. http://doi.org/10.2196/jmir.1867

Kuo, A. M. (2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model. *Journal of Medical Internet Research*, *13*(3). http://doi.org/10.2196/jmir.1867

Lareau, B. S. (2006). *An Engineer ' s Primer on Information Security*.

Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? *Growth Lakeland*, *42*(January), 15–20. http://doi.org/10.1109/MC.2009.20

Liu, J., Huang, X., & Liu, J. (2015). Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. *Future Generation Computer Systems*, *52*, 67–76.

Lober, W. B., Zierler, B., Herbaugh, a, Shinstrom, S. E., Stolyar, a, Kim, E. H., & Kim, Y. (2006). Barriers to the use of a personal health record by an elderly population. *AMIA ... Annual Symposium Proceedings / AMIA Symposium. AMIA Symposium*, 514–518.

Mahajan, a, & Sharma, S. (2015). The Malicious Insiders Threat in the Cloud. *Oaji.Net*, *3*(2), 245–256. Retrieved from http://oaji.net/articles/2015/786-1431229638.pdf

Mahmood, Z., & Hill, R. (2011). *Computer Communications and Networks*.

Maloney, F. L., & Wright, A. (2010). USB-based Personal Health Records: an analysis of features and functionality. *International Journal of Medical Informatics*, *79*(2), 97–111. http://doi.org/10.1016/j.ijmedinf.2009.11.005

Marshall, C. C., & Rossman, G. B. (2011). *Designing Qualitative Research*. (H. Salmon, Ed.) (Sixth). United States of America: SAGE PublicationS.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems*, *51*(1), 176–189. http://doi.org/10.1016/j.dss.2010.12.006

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, *145*, 7.

Ming, L., Shucheng, Y., Kui, R., & Wenjing, L. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. *Lecture Notes of the Institute for Computer Sciences, Social-*

Informatics and Telecommunications Engineering, *50 LNICST*, 89–106. http://doi.org/10.1007/978-3-642-16161-2_6

Mishra, A., Mathur, R., Jain, S., & Rathore, J. (2011). Cloud Computing Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *1*(1), 36–39.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, *63*(2), 561–592. http://doi.org/10.1007/s11227-012-0831-5

Neal, H. (2008). EHR vs. EMR, What's the Difference. Retrieved May 29, 2013, from http://profitable-practice.softwareadvice.com/ehr-vs-emr-whats-the-difference/

Nguyen, D. (2015). Getting Started with Cloud Computing. Retrieved September 10, 2015, from http://codentrick.com/getting-started-with-cloud-computing/

Nikolić, B., & Ružić-Dimitrijević, L. (2009). Risk Assessment of Information Technology Systems. *Issues in Informing Science & Information Technology*, *6*, 595–615. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=aph&AN=44457572&site=ehost-live%5Cn/Users/jamie/SkyDrive/Forensics/CTEC5306/Research/risk assessment of information technology systems.pdf

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Working Papers on Information Systems*, *10*(26), 1–51. http://doi.org/10.2139/ssrn.1954824

Olivier, Martin, S. (2009). *Information Technology Research: A practical guide for Computer Science and Informatics* (Third Edit). Van Schaik. http://doi.org/10.1017/CBO9781107415324.004

Onwubiko, C., Rimal, B. P., Choi, E., & Lumb, I. (2010). Cloud Computing. *Computer Communications*, *77*, 271–288. http://doi.org/10.1007/978-1-84996-241-4

Osterhaus, L. C. (2010). Cloud Computing and Health Information. *U of I SLIS Journal*, *19*, 1–7.

Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. *Bmj*, *335*(7615), 330–333. http://doi.org/10.1136/bmj.39279.482963.AD

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. http://doi.org/10.1016/j.giq.2010.01.002

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. http://doi.org/10.1109/CloudCom.2010.66

Peltier, T. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. crc press.

Pocatilu, P., Alecu, F., & Vetrici, M. (2010). Using Cloud Computing for E-learning Systems 2 Cloud Computing. *WSEAS Transactions on Computers*, *9*(1), 42–51. Retrieved from http://dl.acm.org/citation.cfm?id=1852381.1852386

Puttaswamy, K. P. N., & Zhao, B. Y. (2011). Silverline : Toward Data Confidentiality in Storage-Intensive Cloud Applications. *Access*, 1–13. http://doi.org/10.1145/2038916.2038926

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). Research Methodology. *The Journal of Mathematical Behavior*, *13*(2), 239. http://doi.org/10.1016/0732-3123(94)90027-2

Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in Cloud computing. *Information Security for South Africa (ISSA), 2010*. http://doi.org/10.1109/ISSA.2010.5588290

Reasoning. (n.d.). Merriam-Webster's online dictionary. Retrieved June 24, 2014, from http://www.merriam-webster.com/dictionary/reasoning

Rhodes-Ousley, M. (2013). *The Complete Reference: Information Security* (2nd ed.). McGraw Hill Education.

Robison, J., Bai, L., Mastrogiannis, D. S., Tan, C. C., & Wu, J. (2012). A survey on PHR technology. *2012 IEEE 14th International Conference on E-Health Networking, Applications and Services, Healthcom 2012*, 184–189. http://doi.org/10.1109/HealthCom.2012.6379393

Sabahi, F. (2011). Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 245–249. http://doi.org/10.1109/ICCSN.2011.6014715

Sadgrove, K. (2016). *The Complete Guide to Business Risk Management* (Third). New York, USA: Routledge.

Sai, G., & Gupta, P. (2015). A solution for minimizing Vendor Lock-In problem in Cloud Computing. *International Journal of Advanced Research in Engineering and Management*, *1*(2), 6–9.

Sands, D. Z. (2007). Building the Health e - Patients. *Health Care*.

Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. *2010 IEEE 3rd International Conference on Cloud Computing*, 280–288. http://doi.org/10.1109/CLOUD.2010.22

SATW. (2012). Cloud Computing, *18*, 322. http://doi.org/10.1201/b11149

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). Cloud Computing Security--Trends and Research Directions. *2011 IEEE World Congress on Services*, 524–531. http://doi.org/10.1109/SERVICES.2011.20

Shiels, B. M., & Valley, S. (2009). Malicious insider attacks to rise.

Singh, J. (2014). Cyber-Attacks in Cloud Computing : A Case Study, *1*(2), 78–87.

Singh, V., & Pandey, S. K. (2013). CLOUD SECURITY RELATED THREATS, *4*(9), 2571–2579.

Steele, R., Min, K., & Lo, A. (2012). Personal Health Record Architectures : Technology Infrastructure Implications anf Dependencies. *Journal of the American Society for Information Science and Technology*, *63*(6), 1079–1091. http://doi.org/10.1002/asi

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006

Sunyaev, A., Kaletsch, A., Mauro, C., & Krcmar, H. (2009). Security Analysis of the German Electronic Health Card ' S Peripheral Parts. In *International Conference on Enterprise Information Systems* (pp. 19–26).

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing.

Computer Law and Security Review, *26*(4), 391–397. http://doi.org/10.1016/j.clsr.2010.05.005

Tang, P. . C., Ash, J. S., Bates, D. W., Overhange, M. J., & Sands, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association*, *13*(2), 121–127. http://doi.org/10.1197/jamia.M2025.records

Tansey, O. (2007). Process A Case Tracing and Elite Interviewing : Sampling for Non-probability Process Tracing : Definition. *PS: Political Science and Politics*, *40*(4), 765–772. http://doi.org/10.1017/Si049096507071211

The Workgroup on the National Health Informatics Infrastrusccture (NHII) of the National Committee on Vital and Health Statistics (NCVHS). (2006). *Personal Health Records and Personal Health Record Systems*. D.C Washington.

Torrey, T. (2016). Apomediation and Apomediary - Definitions. New model of how we find health informaion and understand it. Retrieved March 8, 2017, from https://www.verywell.com/apomediation-definition-2615145

Tripathi, A., & Mishra, A. (2011). Cloud computing security considerations. *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1–5. http://doi.org/10.1109/ICSPCC.2011.6061557

van der Westhuizen, E. (2010). *A framework for Personal Health Records in Online Social Networking*. Nelson Mandela Metropolitan University.

Venable, J. R. (2010). Design science research post Hevner et al.: Criteria, standards, guidelines, and expectations. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6105 LNCS*, 109–123. http://doi.org/10.1007/978-3-642-13335-0_8

Wang, D., Zhang, Z., Wang, P., Yan, J., & Huang, X. (2016). Targeted Online Password Guessing : An Underestimated Threat Targeted Online Password Guessing : An Underestimated Threat, (August), 1242–1254. http://doi.org/10.1145/2976749.2978339

Wang, L., Laszewski, G. Von, & Younge, A. (2010). Cloud computing: a perspective study. *New Generation*, *28*, 137–146. Retrieved from http://link.springer.com.e.bibl.liu.se/article/10.1007/s00354-008-0081-5

Wei, J., Pu, C., Rozas, C., Rajan, A., & Zhu, F. (2013). Modelling the runtime integrity of Cloud servers: A scoped invariant perspective. In *Privacy and security of Cloud Computing* (pp. 212–232). London: Springer.

Win, K., Susilo, W., & Mu, Y. (2006). Personal Health Record Systems and Their Security Protection. *Journal of Medical Systems*, *30*(4), 309–315.

Witry, M. J., Doucette, W. R., Daly, J. M., Levy, B. T., & Chrischilles, E. a. (2010). Family physician perceptions of personal health records. *Perspectives in Health Information Management / AHIMA, American Health Information Management Association*, *7*, 1d. Retrieved from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2805556&tool=pmcentrez&rendertype=abstract

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud Computing Research and Development Trend. In *2010 Second International Conference on Future Networks* (pp. 93–97). Ieee. http://doi.org/10.1109/ICFN.2010.58

Zibouh, O., Dalli, A., & Drissi, H. (2016). Cloud computing security through parallelizing fully Homomorphic encryption applied to multi-cloud approach. *Journal of Theoretical and Applied Information Technology*, *87*(2), 300–307.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. http://doi.org/10.1016/j.future.2010.12.006

Appendix A – Publication stemming directly from this research

Mxoli, A., Gerber, M., & Mostert-Phipps, N. (2014, November). Information security risk measures for Cloud-based Personal Health Records. In *Information Society (i-Society), 2014 International Conference on* (pp. 187-193). IEEE.

Information security risk measures for Cloud-based Personal Health Records

Avuya Mxoli[1+2], Mariana Gerber[1] and Nicky Mostert-Phipps[1]

[1]School of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
[2]Smart Systems
Council for Scientific and Industrial Research
Pretoria, South Africa

Abstract—**Personal Health Records (PHRs) provide a convenient way for individuals to better manage their health. With the advancement in technology, they can be stored via Cloud Computing. These are pay-per-use applications offered as a service over the Internet. Similar to other Internet-based technologies, Cloud Computing poses security risks. This paper aims to formulate the implications of Cloud Computing risks on personal health information. A qualitative content analysis was used to analyse literature on Cloud Computing risks to emphasise its implications from a personal health information perspective. Access management, security issues, legal issues and loss of data are some of the risks that negatively impact the storing of PHRs in the Cloud. These can be mitigated by ensuring that only authorized parties are granted access; ensuring that users do not gain access to other users' data and that data remains encrypted; Cloud providers should comply to audits in order to make sure that proper regulations are followed in securing data in the Cloud; and making backups in case of data loss. Using Cloud-based PHRs can improve healthcare. Cloud Providers should work together with PHR providers in order to make sure PHR users can reap these benefits without being too concerned about the associated risks.**

Keywords—Cloud Computing; personal health records; information security risks; privacy; legislation

I. BACKGROUND

A Personal Health Record (PHR) is usually a web-based tool that allows individuals to capture, share, store and process their medical records in one central place [1], [2], [3]. The PHR is typically created, owned, and maintained by the individual and stores a summary of the individual's health information in one convenient place. It allows the individual to better manage his/her health especially if the individual has been diagnosed with a chronic condition such as diabetes and hypertension or diseases such as cancer, tuberculosis, or HIV/AIDS [4]. Depending on functionality, some PHRs allow individuals to set reminders for taking medications and schedule appointments with healthcare providers. They provide the option to make notes of symptoms, track pain and record side effects of medication. PHRs allow an individual to record medical information such as past and current illnesses, allergies, immunizations, medication, procedures, test results, and more [5], [6].

Some offer a variety of reliable health information, which can aid the individual in improving and better managing their health and that of their loved ones [6]. If an individual is being taken care of by a caregiver or family members, some PHRs allow those individuals to have access to some of the person's medical information. This promotes a better collaboration between the individual and those taking care of him.

PHRs enable individuals to provide their healthcare provider with a detailed summary of their medical history. Some allow health care providers to make notes on the individual's condition. Besides speeding up the diagnosis process and eventually the healing process, it could improve continuity of care by providing other healthcare providers with a clear description of the individual's health status based on what other healthcare providers discovered or observed [7]. Consulting with multiple healthcare providers may reduce the chances of having duplicate tests done if an individual uses a PHR [8]. Individuals may also use a PHR at home to monitor chronic diseases [7]. When forwarding PHRs to doctors or caregivers, timely advice and encouragement could be provided to individuals while they are at home recovering.

Web-based PHRs could be stored using Cloud Computing storage facilities [9]. Cloud Computing can be defined as a broad array of pay-as-you-go applications delivered as a service over the internet as well as the hardware and software used in the datacenters that provide the services [10], [11].

Cloud Computing has gained recognition; to such an extent that PHR providers are willing to shift their storage and applications to the Cloud [9]. It has also been claimed that Cloud Computing is set to see immense global investment in many sectors, including health care [12]. There are many ways that patients and healthcare providers can benefit from using the Cloud to access, store and manage PHRs [13], [14], [15], [16], [11], [7]. These include:

The financial assistance of the South African National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

- Reduced cost
- Improved continuity of care
- Interoperability
- Ease of use
- Scalability

Regardless of the many advantages that Cloud-based PHRs offer, the problem is that it also poses security and privacy risks to individuals' PHRs, which typically contain sensitive health information. This paper focuses on the implications of Cloud-based PHRs, by identifying risks to privacy and security of PHRs stored in the Cloud and proposes mechanisms to address these.

II. METHODS

For this research study, a literature study, in combination with a qualitative content analysis was used to identify and analyze relevant literature sources. A literature review was conducted to identify Information Security risks related to Cloud-based PHRs. The identified risks were further analyzed according to Confidentiality, Integrity and Availability as seen on Table 1. Based on this analysis, measures to address these risks were identified. Content analysis is one of the many qualitative methods used to analyze textual data. It focuses on detail and depth rather than measurement [17]. For the purpose of this study, this research method was found to be appropriate.

The next section discusses some Information Security risks and their implications on Cloud-based PHRs, followed by potential ways to address these.

III. INFORMATION SECURITY RISKS RELATING TO CLOUD-BASED PHRS

Health information on its own needs to be protected due to privacy issues; this is amplified when it comes to storing it in the Cloud because of the security and privacy risks that it is exposed to [14]. In general, for PHR's within the Cloud Computing environment, there are concerns around privacy and security. Below are some of these risks. These risks can be grouped according to two categories i.e. unauthorized access and loss of data.

Unauthorized access:

- Malicious insiders: The Cloud provider's staff members who have authorized access to a user's data may misuse it to perform malicious attacks on the users' PHR data [18].
- Physical intrusion: Cloud storage facilities are at a risk of being accessed by intruders which may compromise PHR data stored there [19].
- Third party access: A Cloud provider may decide to outsource the storage of some of their users' data to external parties [20]. This increases the fear of unauthorized access to the user's PHR data [21].
- Multi-tenancy: Different users share memory, networking capabilities etc. in Cloud Computing. This puts users' data at risks of being accessed by malicious attackers posing as PHR owners [22].
- Poor encryption key management: Some systems allow users to generate their own decryption keys and distribute them to authorized parties [14]. This becomes a challenge if the user loses the keys or discloses them to malicious parties [12].
- Software intrusions: A user's PHR may be attacked by malware which can compromise their sensitive information such as login details [23].

Loss of data:

- Data lock-in: It is possible that a PHR provider may want to change Cloud providers due to different reasons. Cloud Computing makes this difficult because most Cloud infrastructures have little capability on data, application and service interoperability [12].
- Systems unavailability: In the Cloud environment there is a possibility of systems unavailability and this can be a major issue in an emergency situation where an individual needs their PHR data [14].
- Temporary outages: Cloud services can and do experience temporary outages which last for hours [24].
- Prolonged and permanent outages: It is possible for a Cloud provider to experience serious problems such as bankruptcy or facility loss. This affects service for extended periods or even leads to a complete shutdown [25].
- Denial of Service (DoS): This involves "saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner" [25]. The attacker is not targeting the information but rather it aims at denying genuine rights to others [26].

The following section categorizes the above mentioned risks according to some aspects of Information Security that can be affected by them.

IV. RISK CATEGORIES

Data security is one of the most recognized problems in Cloud Computing [27], [28]. Information Security may be defined as "something that ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)" [29]. It involves three aspects: confidentiality, integrity and availability (CIA):

- Confidentiality: refers to who has access or authority to access certain information.

- Integrity: refers to the modification of assets by authorized parties and these can be data, hardware or software.
- Availability: refers to whether the data is available when needed by authorized parties.

Table 1 illustrates the classification of the above mentioned risks according to the aspects of CIA. The definition of each identified risk was analyzed to determine the implication of risk according to the aspects to which it most closely relates. Some risks were associated with having implications to more than one aspect.

TABLE I. PHR-RELATED CLOUD COMPUTING RISKS

RISK	Category		
	Confidentiality	***Integrity***	***Availability***
Unauthorized access			
Malicious insiders	✓	✓	✓
Physical intrusion	✓		✓
Third party access	✓	✓	
Multi-tenancy	✓	✓	✓
Poor encryption key management	✓	✓	✓
Software intrusions	✓	✓	✓
Loss of data			
Data lock-in	✓	✓	✓
Systems unavailability			✓
Temporary outages			✓
Prolonged and permanent outages			✓
Denial of Service (DoS)			✓

V. ADDRESSING INFORMATION SECURITY RISK FOR CLOUD-BASED PHRS

This section discusses potential measures that can be taken in order to mitigate the risks mentioned in the Information Security risks relating to PHRs section according the categories mentioned in the one above. The ISO 27799:2008 standard for information security management in health was consulted to identify some of the measures.

A. Unauthorized Access

The following sub-section includes a discussion on addressing risks that may compromise access to an individual's Cloud-based PHR. The risks that fall under this sub-section are malicious insiders, physical intrusion, third-party access, multi-tenancy, poor encryption key management and software intrusions as illustrated on Table 1. Suggestions from various authors are mentioned below [30], [31], [21], [32], [25], [33], [34]:

Personal health information should be uniformly classified as confidential. The following characteristics of information assets need to be considered. Confidentiality of personal health information is:

- Often largely subjective, rather than objective.
- Context-dependent i.e. when used in a different context, information can be confidential whereas in another it may not be.
- Prone to shift over the lifetime of individual's health record. Some issues that are considered confidential currently may not have been considered as confidential in another lifetime.

Because of these characteristics, all personal health information should be subject to suitable protection at all times. Confidentiality, can be compromised if the PHR data is somehow leaked or there is a misapplication of network rights. All health systems used to process personal health information should, therefore, inform users of the confidentiality of the personal health information accessible from such systems, e.g. at start-up or log-in. Hard copy output from the systems should be labeled as confidential (7.4.2.2.). There must be an agreement in place that specifies the confidential nature of the information. It must be applicable to all personnel that have access to the health information (7.3.2.3.). Ways to prevent confidentiality breach include network security controls; network authentication services and data encryption services.

Identity and access management (IAM) can be used to ensure that only the users with the legitimate identity can gain access. Organizations that process personal health information must control access to the information. Users of health information systems should only access personal health information when there is a healthcare relationship between the user and data subject; the user is carrying out activities on behalf of the data subject; or when there is a need for specific data to support this activity (7.8.1.). Identity is crucial to any system that is security conscious. It grants users, services, servers and any other entities access to the system. IAM focuses on Authorization, Authentication and Auditing (AAA) of the users accessing Cloud services. Access to health information systems that contain personal health information must be subject to a formal user registration process. This will ensure that the level of authentication required by the claimed user identity is consistent with the level(s) of access that will be granted to the user. These details must be periodically reviewed to ensure that they are complete, accurate and that the access is still required (7.8.2.1.). This preserves the confidentiality of the system and the data contained therein. Health information systems that process personal health information must authenticate users and should do that by means of authentication that involves at least two factors (7.8.5.1.). Apart from authentication, user privileges should exist and be monitored in order to restrict access to sensitive parts of a system or consumer's data. Role-based access control, workgroup-based access control and discretionary access control can help to ensure confidentiality and integrity (7.8.2.2.). Organizations that process personal health information should clearly define and assign information security responsibilities. They should also have an

Information Security Management Forum (ISMF) that will ensure that there is clear direction and visible management support for initiatives which involve the security of health information (7.3.2.1.). Special consideration, however, should be given in cases where a user may need to access personal health information in an emergency situation where the subject of care may be unable to grant the access (7.8.2.4.). Health information systems processing personal health information must provide personally identifying information that will assist health professionals in confirming that the electronic health record retrieved belongs to the subject of care under treatment (7.9.2.5.).

Integrity, when it comes to information stored in the Cloud, requires that three principles are met i.e.

- Unauthorized personnel or processes cannot make modifications.
- Authorized personnel or processes cannot make unauthorized modifications.
- The data is internally and externally consistent meaning the data stored internally matches all its sub-entities as well as the one stored externally.

Firewall services, communications security management and intrusion detection systems may be used to preserve information integrity. Health information systems that contain personal health information should create a secure audit record every time a user accesses, creates, updates or archives personal health information via the system. The audit log should uniquely identify the user, data subject; identify the action performed by the user and note time and note of such an action. When personal health information has been updated, the original document as well as its audit log should be retained (7.7.10.2.). The integrity of the information contained in the PHR can be maintained by conducting these logs. There should be a segregation of duties and responsibilities in order to reduce chances for unauthorized modification or misuse of personal health information (7.7.1.3.). The availability of PHR data can be compromised if the above mentioned CIA aspects because once confidentiality and integrity are compromised it means a third party gained unauthorized access and by modifying the data they can influence its availability. One way that loss of availability can occur is if an employee changes the name of a file then there will be no way to access it if they do not share this information. Some of the elements that can be used to ensure availability include backups and redundant disk systems; acceptable logins and operating process performance; and reliable and interoperable security processes and network security mechanisms. Below are suggestions that relate specifically to the risks and ISO 27799:2008 controls that relate to each risks are discussed.

I. Malicious insiders

Malicious insiders pose a serious threat to consumer data as they can use a higher level of access to gain access to confidential information about the consumer. They can use this information without the knowledge of the consumer and they can also compromise its availability. An important requirement for Cloud providers is that they monitor their administrators in terms of what they access and a background check should also be conducted. An access control policy must be in place in order to govern access to personal health information. It should be predefined according to the roles with associated authorities, which are consistent, but limited to the needs of that particular role (7.8.1.2.). Prior to employment (7.5.1.), staff members should be given roles and responsibilities in the job description; there should be a screening process to verify identity, living address, previous employment; terms and conditions of employment. During employment (7.5.2.), staff members should be assigned responsibilities; get information security awareness and training; be informed of the disciplinary process. Upon termination or change of employment (7.5.3.), access rights must be revoked. Consumers should then ask their Cloud providers to give them specific details about the people they hire and exactly what kind of privileged access they have over their data. Consumers should demand more transparency from the Cloud providers, in terms of the security and management process including compliance reporting and breach notification.

II. Physical Intrusion

There should also be a physical security perimeter in order to control access to facilities that contain personal health information; there should be physical entry controls; offices should be secured; rooms and facilities should be secured; protection against external and environmental threats should exist; public access, delivery and loading areas should be secure enough not to expose personal health information. These are all there in order to ensure that the public do not get too close IT equipment. Equipment or software used to support a healthcare application that contains personal health information should not be removed from the site or relocated within the organization without authorization by the organization (7.6.).

III. Software intrusion

Appropriate prevention, detection and response controls to protect against malicious software must be adopted and appropriate user awareness training should be implemented (7.7.4.1.). Cloud services have intrusion detection systems (IDSs), intrusion prevention systems (IPSs), virtual private networks (VPNs) and multifactor authentication. These systems set off alerts about detected intrusions then a system administrator or the actual system takes appropriate action.

IV. Third party access

A risk assessment must be carried out by organizations responsible for processing health information to weigh the risks that third parties might pose to the systems and data they contain. Security controls must then be implemented according to the identified level of risk and to the technologies used (7.3.3.1.). In cases where a third party is granted access to process personal health information, there must be formal contracts that specify the confidential nature and value of the personal health information, security measures that must be implemented and/complied with, limitations to access these services by third-parties, the service levels to be achieved in services rendered, the arrangements for compliance auditing of the third-parties, and the penalties that will apply should any of these not be honored (7.3.3.3.). Information exchange agreements that specify the minimum set of controls to be implemented must also be used (7.7.8.1.).

V. Multi-tenancy

Development, test and operation facilities should be separated (physically or virtually) (7.7.1.4.). Compartmentalization should be enforced in order to ensure that consumers may not access other consumers' information due to multi-tenancy. "Policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment" says [35].

VI. Poor encryption key management

Encryption is considered as the main solution to obtaining confidentiality for data, processes and communications. It is one of the solutions to ensuring security in the Cloud. If applied, it is recommended that it be performed at multiple locations, within the data center, or between private and public Clouds and so on. Consumers are also advised to encrypt their data separately before uploading it.

B. Loss of data

This sub-section covers possible measures that can be taken to mitigate risks that relate to data lock-in, systems unavailability, temporary outages, prolonged and permanent outages and Denial of Service (DoS). These risks all relate to the Availability aspect of CIA. Even though it is highly unlikely for Cloud providers to go broke or get acquired and consumed by a larger company, consumers should make sure that their data will remain available [32]. Organizations that process personal health information should carefully assess what impact the loss of network service availability will have on clinical practice (7.7.6.2.) [33]. Below are a few suggestions on how to ensure that data is not lost in the Cloud gathered from [36], [37], [38], [39], [4], [40], [33]:

All personal health information must be backed up and stored in a physically secure environment in order to preserve its future availability. Encryption should be used to preserve confidentiality (7.7.5.). Business continuity management which includes disaster recovery is increasingly recognized as a requirement for health organizations (7.11). In case of a disaster occurring, whether it is of natural or human origin, data in the Cloud should be regularly backed up for recovery. Using the virtualization software, virtual servers can be copied which can provide backups and quick reallocation of computing resources without downtime. Cloud providers can back up their consumer data across a number of Clouds. This will help in the recovery process if one Cloud service fails. The Cloud security alliance [4] proposes that consumers get into a contractual agreement with their Cloud providers which will state the Cloud provider's backup and retention strategies. One of the ways to mitigate data lock-in is the standardization of Application Programming Interfaces (APIs) so that a developer can be able to deploy services and data across many Cloud providers. This will provide a backup in such a way that if there is a failure with one provider, there will still be other copies available. Organizations that process personal health information should report security incidents. These include corruption or unintentional disclosure of personal health information or loss of availability of health information systems, where such a loss undesirably affects patient care (7.10.1.).

Table II summarizes the ISO 27799:2008 controls that can be used to address the specific risks as described above.

TABLE II. PHR-RELATED CLOUD COMPUTING RISKS WITH POTENTIAL ISO CONTROLS

Risk	**Category**		
	Confidentiality	***Integrity***	***Availability***
	ISO 27799:2008 Controls		
Unauthorized access			
Malicious insiders	7.3.2.1. 7.3.2.3. 7.4.2.1. 7.4.2.2. 7.5. 7.7.1.3. 7.7.8.1. 7.7.10.2. 7.8.1. 7.8.1.2. 7.8.2.1. 7.8.2.2. 7.8.5.1.	7.3.2.1. 7.5. 7.7. 7.8.2.2. 7.8.5.1.	7.3.2.1. 7.7.1.3.
Physical intrusion	7.6.		7.6.
Third party access	7.3.2.3. 7.3.3.1. 7.3.3.3. 7.4.2.1. 7.4.2.2. 7.7.8.1. 7.7.10.2. 7.8.1. 7.8.1.2. 7.8.2.1. 7.8.2.2. 7.8.2.4. 7.8.5.1. 7.9.2.5.	7.3.3.1. 7.3.3.3. 7.8.2.2. 7.8.2.4. 7.8.5.1.	

Multi-tenancy	7.7.1.4.	7.7. 1.4.	7.7.1.4.
Poor encryption key management			
Software intrusions	7.7.4.1.	7.7. 4.1.	7.7.4.1.
Loss of data			
Data lock-in			7.7.5.
Systems unavailability			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Temporary outages			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Prolonged and permanent outages			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Denial of Service (DoS)			7.7.5. 7.7.6.2. 7.10.1. 7.11.

VI. CONCLUSION

As much as Cloud-based PHRs introduce advantages, Cloud Computing poses security and privacy risks to an individual's PHR. This paper focused on the implications of Information Security risks on Cloud-based PHRs. Literature sources were used to highlight the risks that Cloud Computing poses on Cloud-based PHRs as well as potential mechanism to address these risks. Legislation proves to be very significant in enforcing compliance from Cloud providers to protect the data that they store for their consumers. Future research includes developing an approach that will address information security legislation relating to Cloud-based PHRs.

REFERENCES

[1] D C Kaelber, A K Jha, D Johnston, B Middleton, and D W Bates, "A reserach agenda for personal health records," J Am Med InformAssoc, vol. 15, pp. 729-736, 2008.

[2] C Pagliari, D Detmer, and P Singleton, "Potential of electronic personal health records," BMJ, vol. 335, no. 330, pp. 330-333, 2007.

[3] A Sunyaev, D Chornyi, C Mauro, and H Krcmar, "The evaluation framework for personal health records: Microsoft HealthVault vs. Google Health," in System Sciences (HICSS), 2010 43rd Hawaii International Conference, Honolulu, 2010, pp. 1-10.

[4] N Archer, U Fevrier-Thomas, C Lokker , K A McKibbon, and S E Straus, "Personal health records: a scoping review," J Am Med Inform Assoc, vol. 8, no. 4, pp. 515-522, 2011.

[5] H Neal. (2008, November) EHR vs PHR- What's the difference? [Online]. http://profitable-practice.softwareadvice.com/ehr-vs-emr-whats-the-difference/. Access Date: 29 May 2013).

[6] P C Tang, J S Ash, D W Bates, J M Overhange, and D Z Sands, "Personal health records:definitions,benefits, and strategies for overcoming barriers," J AM Med Inform Assoc, vol. 13, no. 2, pp. 121-126, 2006.

[7] The Workgroup on the NHII of the NCVHS, "Personal health records and personal health record systems," Washington,D.C., 2006.

[8] M I Kim and K B Johnson, "Personal health records: Evaluation of Functionality and Utility," Journal of the American Medical Informatics Association, vol. 9, no. 2, pp. 171-180, 2002.

[9] L Ming, Y Shucheng, R Kui, and L Weinjing, "Securing Personal Health Records in CloudComputing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in Security and privacy in communication networks.: Springer Berlin Heidelberg, 2010, pp. 89-106.

[10] F Sabahi, "Cloud computing security threats and responses," in Communicayion software and networks (ICCSN),2011 IEEE 3rd International Conference, 2011, pp. 245-249.

[11] J Geelan. (2009, January) Twenty-one experts define cloud computing. [Online]. http://virtualization.sys-con.com/node/612375. Access Date: 18 February 2014).

[12] A Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model," Journal of Medical Internet Research, vol. 13, no. 3, pp. 622-645, 2011.

[13] S Marston, Z Li, S Bandyopadhyay, J Zhang, and A Ghalsasi, "Cloud computing-the business perspective," Decision support systems, vol. 51, no. 1, pp. 176-189, 2011.

[14] E Abukhousa, N Mohamed, and J Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges.," Future Internet, vol. 4, no. 3, pp. 621-645, 2012.

[15] S Zhang, S Zhang, X Chen , and X Huo, "Cloud computing research and development trend," in 2010 second Internation Conference on Future Networks, Sanya, 2010, pp. 93-97.

[16] M E Bégin et al., "An EGEE comparative study: Grids and Clouds-Evolution or Revolution," 2008.

[17] J Forman and L Damschroder, "Qualititative methods," in Empirical methods for bioethics: A primer, 11th ed., L Jacoby and L A Siminoff, Eds. Oxford: Elsevier, 2008.

[18] A Behl, "Emerging Security Challenges in Cloud Computing: An insight to cloud security challenges and their mitigation," in Information and Communication Technologies (WICT), Mumbai, 2011, pp. 217-222.

[19] A Hutchings, S G Russell, and J Lachlan, "Cloud computing for small businesses: criminal and security threats and prevention measures," Trends and issues in Crime and Criminal Justice, no. 456, pp. 1-8, 2013.

[20] D Zissis and D Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2012.

[21] C Modi, D Patel, B Borisaniya, A Patel, and M Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561-592, 2013.

[22] A Mishra, R Mathur, S Jain, and J S Rathore, "Cloud computing security," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, no. 1, pp. 36-39, 2013.

[23] J Wei, C Pu, C V Rozas, A Rajan, and F Zhu, "Modelling the runtime integrity of Cloud servers: A scoped invariant perspective," in Privacy and security of Cloud Computing, S Pearson and G Yee, Eds. London: Springer, 2013, pp. 212-232.

[24] N Leavitt, "Is Cloud Computing Really Ready for Prime Time?," Computer, vol. 42, no. 1, pp. 15-20, 2009.

[25] W A Jansen, "Cloud hooks: security and privacy issues in Cloud computing," in System sciences (HICSS),2011 44th Hawaii INternational Conference, 2011, pp. 1-10.

[26] K T Win, W Susilo, and Y Mu, "Personal Health Record Systems and Their Security Protection," Journal of Medical Systems, vol. 30, no. 4, pp. 309-315, 2006.

[27] A Sarwar, M Naeem, and A Khan, "A Review of Trust Aspects in Cloud Computing Security," International Journal of Cloud Computing and Services Sciences, vol. 2, no. 2, pp. 116-122, 2013.

[28] D Jamil and H Zaki, "Cloud computing security," Internationa Journal of Engineering Science and Technology, vol. 3, no. 4, pp. 3478-3483, 2011.

[29] ISACA, "COBIT 5 for Information Security," ISACA, USA, Preview version 2012.

[30] A Bouayad, A Blilat, N El Houda Mejhed, and M El Ghazi, "Cloud computing:security challenges," in Information Science and Technology (CIST), 2012 Colloquium, 2012, pp. 26-31.

[31] G Kulkarni, J Gambir, T Patil, and A Dongare, "A security aspect in Cloud Computing," in Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference, 2012, pp. 547-550.

[32] J. Brodkin. (2009, July) Network World. [Online]. www.networkworld.com/news/2008/070208-cloud.html?page=1. Access Date: 20 February,2014).

[33] International Organization for Standardization, "Health informatics — Information security management in health using ISO/IEC 27002," Switzerland, eStandard ISO 27799:2008(E), 2008.

[34] C Lo, C Huang, and J Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," in Parallel processiong workshops,2010 39th International conference, San Diego, 2010, pp. 280-284.

[35] H Takabi, J B Joshi, and A Gail-Joon, "SecureCloud:Towards a comprehensive framework for cloud computing environments," in Computer Software and Applications Conference Workshop (COMPSACW),2010 IEEE 34th Annual, 2010, pp. 393-398.

[36] J M Kizza, "Cloud computing and related security issues," in Guide to computer network security. London: Springer London, 2013, pp. 465-489.

[37] S Subashini and V Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[38] K Popovic and Z Hocenski, "Cloud computing security issues and challenges," in MIPRO,2010 Proceedings of the 33rd International Convention, 2010, pp. 344-349.

[39] M A AlZain, E Pardede, B Soh, and J A Thom, "Cloud computing security: from single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference, 2012, pp. 5490-5499.

[40] M Armbrust et al., "A view of Cloud Computing," Communications of the CAM, vol. 53, no. 4, pp. 50-58, 2010.

Appendix B - Other closely related publications

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2014). Personal health records in the South African healthcare landscape: a socio-technical analysis. *International Development Informatics Association Conference, Port Elizabeth, 3-4 November 2014*

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2014). Personal Health Records: Design considerations for the South African context. In: *DDR 2014, Cape Town, 8-10 September 2014*

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2015). Personal Health Records in the South African Healthcare Landscape: A SWOT Analysis. In J. Steyn and D. van Greunen (Eds) *ICTs for Inclusive Communities in Developing Societies* (pp. 344-357). Newcastle upon Tyne, NE6 2PA, UK: Cambridge Scholars Publishing.

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2016). Risks and benefits of social computing as a healthcare tool. In: *International Conference on Society and Information Technology 2016,Orlando, 8-11 March 2016*

Personal Health Records in the South African Healthcare Landscape: A Socio-Technical Analysis

Avuya Mxoli
Nelson Mandela Metropolitan University
Council for Scientific and Industrial Research
South Africa

Nicky Mostert-Phipps
Nelson Mandela Metropolitan University
South Africa

Mariana Gerber
Nelson Mandela Metropolitan University
South Africa

Abstract

Personal Health Records (PHRs) offer various advantages for individuals making use of these systems to document and maintain information related to their health. In addition, PHRs may play a positive role in preventative care and efforts to prevent and control non-communicable lifestyle diseases. Despite numerous benefits adoption rates are low, and little is known regarding the factors that affect adoption in the South African context.

This exploratory paper highlights socio-technical factors that can affect the adoption of PHRs in the South African context. Socio-Technical Systems theory is applied as a theoretical lens to identify the social, technical, and environmental factors that can affect the adoption of PHRs. Factors that can positively contribute to, as well as negatively inhibit, the adoption of PHRs are identified.

Keywords
Personal Health Records, Socio-Technical Systems Theory, South Africa

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.
ISBN: 978-0-620-63498-4 Pages 297-306

Introduction

Costs related to caring for patients with preventable lifestyle diseases are placing an enormous strain on South Africa's struggling healthcare system (Watermeyer, 2013). Patients with hypertension and diabetes account for approximately 17 million visits to healthcare centers in South Africa each year, resulting in significant healthcare costs and use of human resources. As a result, the South African Department of Health has implemented a strategic plan to prevent and control non-communicable diseases. One of the strategies relates to increasing health awareness and healthy lifestyle promotion (Watermeyer, 2013). With the imminent implementation of the National Health Insurance (NHI) in South Africa, there will also be a shift towards offering more effective preventative care as opposed to the South African healthcare system that is currently highly hospital-centric with a strong curative focus (Department of Health, 2011).

A Personal Health Record (PHR) is an electronic application, usually web-based, that allows an individual to document and maintain information related to his own health. PHRs can play a significant role in promoting health and supporting healthcare providers in offering more effective preventative care (Lehmann, et al., 2006; Markle Foundation, 2004; Sprague, 2006). Despite well-documented benefits associated with the adoption and use of PHRs, adoption rates are typically low, especially in developing countries (Dohan, Abouzahra, & Tan, 2014).

Little is known regarding the factors that can affect the adoption and meaningful use of PHRs in the South African context. This exploratory paper will highlight such socio-technical factors. Socio-Technical Systems theory will be applied as a theoretical lens to identify the social, technical, and environmental factors that can affect the adoption of PHRs in the South African context.

The next section will describe the concept of a Personal Health Record in more detail.

Personal Health Records

A Personal Health Record (PHR) is a patient-oriented electronic record, usually web-based, that allows an individual to manage his own healthcare and contains his health related information that has been gathered from many sources (Christopherson, 2005; Sprague, 2006; Tang, Ash, Bates, Overhage, & Sands, 2006). The PHR is typically owned, created, and managed by the individual and allows him to have a lifelong summary of all of his health information in one convenient place. A PHR should typically contain information on past and current illnesses, allergies, immunizations, medication, procedures, tests results, and more (Tang et al, 2006). This is especially useful for individuals who manage chronic conditions such as diabetes and hypertension or diseases such as cancer, tuberculosis, or HIV/AIDS (Markle Foundation, 2004).

General benefits associated with the use of PHRs include the following (Markle Foundation, 2004; Tang el al. 2006):

- Empowering individuals and their families by:
  - Providing them with relevant and credible information to gain a deeper understanding of the health issues and decisions they face.

    - Enabling them to assume a greater responsibility for their care and share in the decision-making process.
    - Monitoring important indicators such as blood pressure, symptoms, glucose levels, and so forth. This is especially beneficial for individuals managing chronic conditions.
    - Providing a way for individuals to involve friends and family in their care when necessary.
    - Reminding individuals to schedule relevant preventative services.
- Improving the relationship between a patient and healthcare provider by improving both communication and the sharing of information.
- Increasing patient safety by alerting patients and healthcare providers of potential drug interactions, contraindications, side effects, and allergies, and alerting them to missed procedures and lapses in adherence to treatment regimes.
- Improving the quality of care that patients receive by providing the healthcare provider with a more complete history of the patient and increasing the understanding of and engagement with treatment plans by the patient.
- Improving the outcomes of care for patients with chronic conditions.
- Promoting earlier interventions when patients with chronic conditions encounter a problem.

Despite these benefits associated with PHRs, adoption rates are typically low, especially in developing countries. Socio-Technical Systems theory will be applied as a theoretical lens to identify the social, technical, and environmental factors that can affect the adoption of PHRs in the South African context.

Theoretical Lens: Socio-Technical Systems Theory

Socio-Technical System (STS) theory has its roots in the field of work redesign and is based on the premise that people (the social subsystem) make use of tools, techniques, and knowledge (the technical subsystem) to achieve a specific task and is open to outside influences from the greater environment in which they operate (the environmental subsystem) (Scacchi, 2004). The STS approach provides significant insights into the interrelationship between people and technology, as well as the influence of the external environment on this interrelationship (Baxter & Sommerville, 2011; Scacchi, 2004). As such, the STS approach is considered as a powerful framework through which the contributors to adoption and meaningful use of many ICT systems can be investigated (Coiera, 2007).

Whilst PHRs are consumer-oriented tools, Nazi (2013) states that PHR use have far-reaching implications for healthcare providers and the greater healthcare system. He also stresses the importance of studying PHR technology as a social practice that is influenced by, and has an influence on, the greater healthcare landscape. STS theory is thus deemed an appropriate theoretical lens through which to investigate factors that may both inhibit, as well as positively contribute, to the adoption and meaningful use of PHRs in the South African context.

Phase 1 of the data collection and analysis focused on identifying literature related to PHRs in the South African context. Only two recorded studies that focus on South African consumers' perceptions towards PHRs could be identified by the authors (Pottas & Mostert-Phipps, 2013; Jojo & Mostert-Phipps, 2013). Relevant South African literature and

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.
ISBN: 978-0-620-63498-4 Pages 297-306

statistics related to access to technology and so forth were also consulted. Based on this literature review several factors that may inhibit/contribute to PHR adoption in the South African context were identified.

In Phase 2 of the data collection and analysis STS theory was applied as a theoretical lens. All identified factors were analysed to determine whether the factor should be classified as a social, technical, or environmental inhibitor/contributor to PHR adoption in the South African context. The following were considered in terms of the STS analysis:

- **Social subsystem:** The influence of consumers on the adoption and meaningful use of PHRs was considered in terms of the analysis of the social subsystem. PHRs are typically owned, created, and managed by an individual, and as such consumers are considered the main roleplayers in the social subsystem.
- **Technical subsystem:** Since PHRs are typically web based, factors related to Internet access, Internet literacy, and so forth were considered in the analysis of the technical subsystem.
- **Environmental subsystem:** Factors related to outside influences that could inhibit or contribute to the adoption of PHRs were considered in the environmental analysis. This includes the influence of government policies, the South African healthcare landscape, and so forth.

Social, technical, and environmental factors that may contribute to or inhibit the adoption and meaningful use of PHRs will be discussed in the sections that follow.

Social Analysis

Since a PHR is typically owned, created, and managed by an individual, the influence of consumers on the adoption and meaningful use of PHRs will be considered in terms of the social analysis. Only two recorded studies that focus on South African consumers' perceptions towards PHRs could be identified by the authors. In 2012 a survey was conducted in the Nelson Mandela Bay (NMB) area of South Africa that investigated the perceptions of consumers regarding PHRs (Pottas & Mostert-Phipps, 2013). A similar nation-wide survey was conducted in 2013 (Jojo & Mostert-Phipps, 2013). Social factors that could inhibit and contribute to the adoption of PHRs in the South African context as derived from the results of these studies are described below.

Social inhibiting factors:

The results of the studies mentioned above indicate the following social factors that may contribute to a lack of adoption and meaningful use of PHRs in the South African context:

- **Personal record keeping practices:** The study conducted in the NMB area indicated that most participants (69%) did not keep a record of their full medical history. Those participants that did keep a record of their medical history primarily made use of paper-based means. The study also indicated that it was more likely for participants with chronic medical conditions to keep a record of their medical history.
- **Lack of awareness:** In the NMB survey, participants were asked if they were aware of the exince of PHRs that could aid them in keeping track of their full medical history and 84% of participants indicated that they were not aware of the existence of PHRs before participating in the survey.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.
ISBN: 978-0-620-63498-4 Pages 297-306

Social contributing factors:

The South African-based studies further indicated the following results that may positively contribute to the adoption and meaningful use of PHRs in the South African context:

- Importance of medical history knowledge: In the national survey, 70% of participants indicated that it is extremely important for their healthcare provider to be aware of their full medical history whilst 42% indicated that their healthcare provider was not informed of their full medical history.
- Benefits offered by PHRs: Once they were made aware of the existence of PHRs, participants in the national survey expressed great interest in the features of web-based PHRs, especially viewing their medical records, test results and educational materials related to their health, as well managing medication lists, setting reminders for preventative health services and communicating with their healthcare providers. 69% of the participants indicated that they are interested in making use of PHRs to view their health information and manage their healthcare.
- Willingness to pay for PHR use: As seen in Figure 1 below, it was encouraging to note that participants in the national survey expressed a willingness to pay a monthly fee for the use of a PHR.

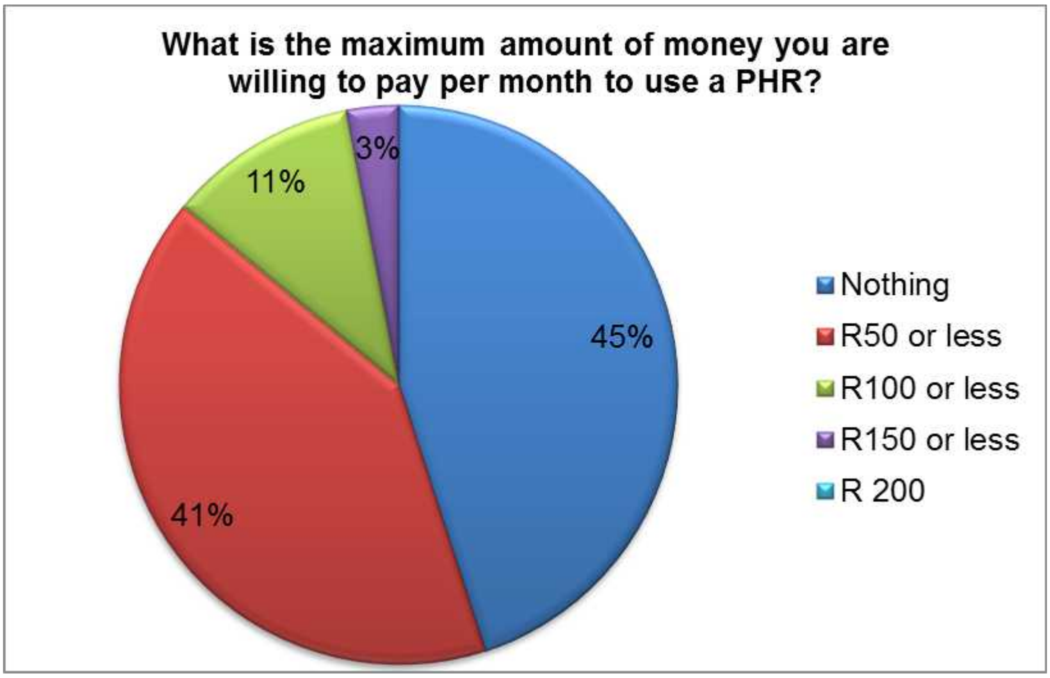


Figure 1. Willingness to pay for PHR use.

- Improved communication with healthcare providers: Participants in the national survey indicated that PHRs could potentially improve communication between themselves and their healthcare providers, with 48% indicating a great improvement, 31% a slight improvement, 13% no effect on communication and only 8% indicated that PHRs could potentially worsen communication.
- Improved understanding of own health: 53% of the participants in the national survey indicated that they believe that PHRs could greatly improve their understanding of matters related to their own health and 28% indicated a possible

slight improvement in understanding.
- Improved sense of control: Participants in the national survey indicated that PHRs could give them an improved sense of control over their own healthcare (53% greatly improve and 30% slightly improve).

In the next section, technical factors that could inhibit and contribute to the adoption of PHRs are described.

Technical Analysis

Since PHRs are typically web-based, Internet access is a requirement for the adoption and meaningful use of PHRs. Other technical factors that may affect the adoption and meaningful use of PHRs include Internet literacy levels and so forth. Technical factors that could inhibit and contribute to the adoption of PHRs in the South African context are described below.

Technical inhibiting factors:

- Internet access: Statistics from Statistics South Africa's General Household Survey for 2013 reveal that access to the Internet remains a problem in South Africa (Statistics South Africa, 2013). As seen in Table 1, while the statistics vary from one province to the next, on average only 10% of South African households have access to the Internet at home (Statistics South Africa, 2013). When considering access to the Internet outside the home, the statistics further revealed that for 16.1% of households at least one member of the household has access to the Internet at home and 9.6% at Internet cafes or educational facilities. These statistics exclude access to the Internet via mobile devices such as cellular phones or 3G cards.

Place Internet is accessed	**Province (%)**									
	WC	**EC**	**NC**	**FS**	**KZN**	**NW**	**GP**	**MP**	**LP**	**RSA**
At home	21.0	4.8	6.6	6.9	5.7	4.4	15.6	6.8	3.0	**10.0**
At work	24.4	9.5	10.2	10.4	11.5	8.6	27.5	8.5	4.9	**16.1**
Using mobile devices	35.4	24.4	32.5	34.3	25.3	30.9	38.3	31.9	16.5	**30.8**
At Internet cafes or educational facilities	16.7	5.1	3.1	10.0	7.1	7.1	15.1	4.8	1.6	**9.6**

Table 1. SA Household Internet access by place of access (Statistics South Africa, 2013).

- **Internet literacy:** The national survey referred to in previous sections indicated that participants in that survey did not rate themselves as particularly Internet literate (Pottas & Mostert-Phipps, 2013). When asked to rate their Internet literacy level, less than half of the participants considered themselves to be 'skilled' or 'very skilled' in terms of navigating the Internet to search for information (45%) and uploading and downloading information (47%).

Slightly more participants (52%) rated themselves as ‘skilled’ or ‘very skilled’ in terms of their ability to send e-mails.

- **Privacy concerns:** In the NMB survey mentioned previously the majority of participants (58%) indicated that they would be concerned about the privacy of their personal health information when using a PHR (Pottas & Mostert-Phipps, 2013).

Technical contributing factors:

- Access to mobile technology: Statistics South Africa’s General Household Survey for 2013 reveal that at least 81.9% of South African households had access to at least one cellular phone (Statistics South Africa, 2013). As shown in Table 1, it is also encouraging to note that mobile technology has made access to the Internet much more accessible to South African households with 30.8% of households having mobile access to the Internet (Statistics South Africa, 2013).

As mentioned, PHRs have far-reaching implications for healthcare providers and the greater healthcare system and as such environmental factors that may contribute to or inhibit the adoption and meaningful use of PHRs will be discussed in the next section.

Environmental Analysis

Since this study focused on identifying factors through a literature review that focused on the South African context only, no environmental inhibiting factors could be identified. This does not imply that there are no environmental factors that could potentially inhibit the adoption and meaningful use of PHRs in the South African context, but it does indicate that it is a research area that has received little attention. The section below highlights environmental factors that may positively contribute to the adoption and meaningful use of PHRs in the South African context.

Environmental contributing factors

National Health Insurance (NHI): Once the National Health Insurance (NHI) is implemented in South Africa, primary healthcare services will be re-engineered to focus mainly on health promotion and preventative care (Department of Health, 2011). PHRs can play a significant role in achieving these goals by enabling patients to better manage their healthcare (Sprague, 2006). PHRs could be utilized to better educate patients about their medical conditions, improve adherence to medical and lifestyle changes, and engage them in medical decision-making. Its role in increasing health awareness could prove invaluable in promoting health and supporting healthcare providers in offering more effective preventative care as opposed to the South African healthcare system that is currently highly hospital-centric with a strong curative focus (Department of Health, 2011; Lehmann, et al., 2006; Markle Foundation, 2004).

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.
ISBN: 978-0-620-63498-4 Pages 297-306

- **Managing and reducing costs:** The use PHRs may gain support from healthcare funders since it may reduce healthcare costs due to fewer admissions and emergency room visits, avoidable drug-drug interactions, avoidable over-use of medications and increased use of over-the-counter medication in treating common chronic conditions (Adão, 2013).
- **Improved quality of healthcare:** Participants in the national survey mentioned previously perceived PHRs to contribute to an improvement in the healthcare that they receive with 45% indicating a potential great improvement and 33% a slight improvement. Participants also indicated that PHRs can contribute to a reduction in medical errors due to a lack of information, with 37% indicating a potential great improvement and 38% a slight improvement.

Discussion

The results of this study have revealed that whilst there are many factors that may positively contribute to the adoption and meaningful use of PHRs by South African consumers, there are also some significant barriers. The greatest of these being a lack of awareness in terms of the existence of PHRs and the benefits offered by PHR use, as well as a lack of access to the Internet through traditional channels. Despite the results that indicate a lack of Internet access as a significant barrier, emerging mobile PHRs (mPHRs) hold great promise to encourage the adoption and meaningful use of PHRs as a platform to engage South African consumers in self-care (Adão, 2013). Statistics also indicate that significantly more South African households have access to the Internet via mobile devices than through any other means, as previously seen in Table 1 (Statistics South Africa, 2013).

Conclusion

This exploratory study focused only on literature relating to the South African context in an effort to identify socio-technical factors that may inhibit or positively contribute to the adoption and meaningful use of PHRs by South African consumers. There are limited published studies related to the adoption and meaningful use of PHRs in the South African context. The socio-technical analysis discussed in this paper provides insights into the interrelationship between the various role-players involved in the adoption of PHRs, as well as the influence of such role-players on the successful adoption of PHRs. Whilst this paper highlighted various barriers that should be addressed to support the adoption of PHRs, it is encouraging to note that consumers (social subsystem) are very interested in the features offered by PHRs and that there are various environmental factors that may also contribute to the successful adoption of PHRs in the South African healthcare landscape.

This study further revealed that there is a need for further research to identify comprehensive factors that may inhibit or positively contribute to the adoption and meaningful use of PHRs in the South African context. Future research will focus on identifying such factors, as well as investigating the relevance of international literature on the topic in the context of the South African healthcare landscape.

Acknowledgements

The financial assistance of the South African National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

Adão, W. (2013, May 27). *Technology enabled self-care to overhaul healthcare industry.* Last accessed June 26, 2014, from Deloitte: http://www.cover.co.za/healthcare/technology-enabled-self-care-to-overhaul-healthcare-industry

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4 - 17.

Christopherson, G. A. (2005). HealthePeople: Person-Centered, Outcomes-Driven, Virtual Health Systems. In J. E. Demetriades, R. M. Kolodner, & G. A. Christopherson, *Person-Centered Health Records: Toward HealthePeople.* Springer.

Coiera, E. (2007). Putting the technical back into socio-technical research. *International Journal of Medical Informatics*, 98 - 103.

Department of Health. (2011). National Health Act (61/2003): Policy on National Health Insurance. *Government Gazette, 554*(34523).

Dohan, M. S., Abouzahra, M., & Tan, J. (2014). Mobile Personal Health Records: Research Agenda for Applications in Global Health. *47th International Conference on System Science,* 2576 - 2585. Hawaii: IEEE.

Jojo, S., & Mostert-Phipps, N. (2013). Awareness and interest in web-based Personal Health Records. *Proceedings of the 15th Annual Conference on World Wide Web Applications.* Cape Town: Cape Peninsula University of Technology.

Lehmann, H. P., Abbott, P. A., Roderer, N. K., Rothschild, A., Mandell, S., Ferrer, J. A., et al. (2006). *Aspects of Electronic Health Records* (2nd ed.). Springer.

Markle Foundation. (2004, July). Last accessed June 10, 2014, from Connecting Americans to their Healthcare: Working Group on Policies for Electronic Information Sharing Between Doctors and Patients:
http://www.markle.org/sites/default/files/eis_exec_sum_final_0704.pdf

Nazi, K. M. (2013). The Personal Health Record Paradox: Health Care Professionals' Perspectives and the Information Ecology of Personal Health Record Systems in Organizational and Clinical Settings. *Journal of Medical Internet Research, 15*(4).

Pottas, D., & Mostert-Phipps, N. (2013). Citizens and Personal Health Records - The Case of Nelson Mandela Bay. Studies in Health Technology and Informatics, 192, 501-504. IOS Press.

Scacchi, W. (2004). Socio-technical design. In W. S. Bainbridge (Ed.), *The Encyclopedia of Human-Computer Interaction.* Berkshire Publishing Group.

Sprague, L. (2006). *Personal Health Records: The People's Choice?* Last accessed June 10, 2014, from National Health Policy Forum. Issue Brief Number 820. : URL: http://www.nhpf.org/library/issue-briefs/IB820_PHRs_11-30-06.pdf.

Statistics South Africa. (2013). *General Household Survey 2013.* Last accessed June 26, 2014, from http://beta2.statssa.gov.za/publications/P0318/P03182013.pdf

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association, 13*(2), 121-126.

Watermeyer, L. (2013, 9 18). *Health-e*. Last accessed June 27, 2014, from Government unveils NCD startegic plan: http://www.health-e.org.za/2013/09/18/government-unveils-ncd-strategic-plan/

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.
ISBN: 978-0-620-63498-4 Pages 297-306

Risks and Benefits of Social Computing as a Healthcare Tool

Avuya MXOLI
School of Information and Communication Technology,
Nelson Mandela Metropolitan University,
Port Elizabeth,
Eastern Cape,
South Africa.
Command, Control and Information Warfare unit,
Council for Scientific and Industrial Research,
Pretoria,
Gauteng,
South Africa

Nicky MOSTERT-PHIPPS
School of Information and Communication Technology,
Nelson Mandela Metropolitan University,
Port Elizabeth,
Eastern Cape,
South Africa

and

Mariana GERBER
School of Information and Communication Technology,
Nelson Mandela Metropolitan University,
Port Elizabeth,
Eastern Cape,
South Africa

ABSTRACT

Cybercitizen describes a frequent user of the Internet or in other terms, a member of an online community (cybercommunity). This digital space can be used to participate in educational, economical and cultural activities. Social computing is an approach to Information Technology (IT) that is used to create virtual teams across different organizations or communities which enhances collaboration, collection and sharing of information. It allows different stakeholders to come together in order to communicate and share information in a more effective way using cybercommunities. Individuals are increasingly making use of social computing applications as healthcare tools.

This paper describes how social computing applications are being used as healthcare tools. Benefits associated with such use are described and the risks highlighted. This information may help raise awareness in terms of the benefits that individuals and medical professionals can reap from employing social computing applications as healthcare tools, whilst also cautioning them to consider the risks associated with such use.

Keywords: Social computing, cybercommunity, cyber world, healthcare, risks, benefits

1. INTRODUCTION

Human beings are naturally societal and thus require relationships with others in order to survive [1]. This can be witnessed in the need for having a place to belong or a certain group of people to relate to. Social computing is an approach to Information Technology (IT) that is used to create virtual teams across different organizations or communities which enhances collaboration, collection and sharing of information [2]–[4]. It allows different stakeholders to come together in order to communicate and share information in a more effective way using cybercommunities. Social computing has made this easier because these social connections are no longer limited to physical contact but they can occur in the cyber world as well. It has been found that many individuals are increasingly relying on social computing to access health information or to track their health conditions and care [5], [6].

The purpose of this paper is to highlight the concept of social computing as a healthcare tool, as well as define the risks and benefits of social computing as a healthcare tool. In this paper, social computing will be defined and described, the application of social computing as a healthcare tool will be discussed, and the benefits and risks associated with it will be highlighted. The results presented in this paper are based on a literature review. The paper ends with a brief discussion and future work.

2. SOCIAL COMPUTING

The Internet used to be just a "read-only" service which had little user interaction, also referred to as Web 1.0 [7], [8]. However, things have evolved and now people can read and contribute to content on the Internet – allowing interaction and collaboration [7]. This is known as Web 2.0 and social computing falls under it. Some of the essential characteristics of social computing include the following [3], [8]–[10]:

- **Connectivity:** This is about the formation of relations with people in a group.
- **Collaboration:** This is the sharing of resources, ideas, knowledge experiences in a cyber-community. This can be experienced as both negative and positive. Positive collaboration can be experienced when people collaborate in order to facilitate one another. Negative collaboration on the other hand is when it becomes adversarial or competitive.
- **Community:** This is the grouping of people who have similar interests and may be of spatial closeness.

There are various applications of social computing. The following are examples of such applications [1], [4], [8]–[13]:

- **Blogs:** This is typically a personal diary that is kept in cyber space where an end-user can edit it without requiring web publishing skills. An example of a blog service provider is Blogger (www.blogger.com).
- **Social games:** This is an online activity whereby users play an online game on a social media platform e.g. The Sims (www.thesims.com.thesims.com).
- **Social networks:** Websites that provide social interaction for users to be able to develop groups of friends or communities of people with common interests e.g. Facebook (www.facebook.com).
- **Social media:** Audio or video content is uploaded by individuals on the Internet in order to create a platform for sharing and discussion e.g. YouTube (www.youtube.com).
- **Social knowledge sharing:** On the Internet, users come together across geographic confines to contribute to a collective pool of knowledge e.g. Wikipedia (en.wikipedia.org).

As mentioned it has been found that many individuals are increasingly relying on social computing to access health information or to track their health conditions and care [5], [6]. Social computing as a healthcare tool will be discussed in more detail in the following section.

3. SOCIAL COMPUTING AS A HEALTHCARE TOOL

The combination of social computing applications and health gave rise to the concept of Health 2.0 [6]. This can be defined as a network of Web 2.0 applications that empower the user to take control of their healthcare [7], [14], [15]. It is about availing information to patients which will assist them in making rational and informed healthcare decisions. With the rise of social computing technology, patients are looking for ad-hoc ways to connect to one another and share their healthcare experiences [14]. Hospitals and other health organizations also use social computing for promotions and gauging consumer experiences [5]. Social computing connects patients, doctors, caregivers and other healthcare providers to help them interact actively in the care of a patient. Below are examples of social computing applications and how they can be used as a healthcare tool.

- **Blogs:** Patients use blogs in order to share their stories and empower one another outside the doctor's office [14], [16]. Bloggers use their sites to share the knowledge they have about diseases and illnesses and also raise awareness and educate others on treatment options and where to get useful resources [14].
- **Social games:** The nature of online social games promotes potential learning environments as they are very captivating and engaging [13]. Due to increased access to the cyber world through mobile devices, it is expected that the application of casual gaming will be increasingly leveraged to drive health behaviour change [17].
- **Social networks:** Social networks/peer networks are formed around diseases through health communities in order to provide support groups, and self-help groups [18], [19]. They can help patients in the decision making process and also dealing with consequences of those decisions [15]. Patients with chronic conditions can cope better by using social networks to communicate with other patients to discuss symptoms and treatments [18], [19].
- **Social media:** Podcasts and live video feeds are used to deliver new health information to patients and healthcare providers in a universal manner [16].
- **Social knowledge sharing:** Tools such as medical wikis also exist on the Web. Patients can get disease-specific information from them, which can help in getting more information about their symptoms [16].

In the section that follows, the benefits of social computing applications as healthcare tools will be described.

3.1. Benefits of social computing applications in healthcare

The following benefits related to the social computing applications discussed in the preceding section have been identified [13], [14], [16], [18], [20]–[23]:

- **Blogs:** The participants of blog websites get first-hand information from healthcare professionals and also from other patients that share their experiences on such blogs. Another advantage of blogs is that they are easy to use, because they are just like diaries/journals written online.
- **Social games:** When playing social games that are health-related, patients can get better access to information and support through pre-programmed education modules. Social games also promote behavior change with positive feedback for patients. They are also motivational for young people who are difficult to influence when dealing with health problems. Games can also play a role in improving players' moods, promoting relaxation and warding off anxiety.
- **Social networks:** Patients gain a psychological sense of community as they meet virtually with others to share experiences and gain knowledge on health topics they are interested in. This also helps to fight social isolation because online they feel like they belong to a certain group and thus are never alone in dealing with their health problems.
- **Social media:** Podcasts provide continuous and personalized education and training for medical professionals that are in remote areas. They are also used to deliver educational material to patients related to health, nutrition, and wellbeing. The World Health Organization also makes use of podcasts to distribute public health information and related news from around the world.
- **Social knowledge sharing:** Health and medical wikis are an example. They provide quick updates on what is current in the health domain. Wikis are also used in medical education by students to share web resources and links.

In the following section the risks related to social computing applications as healthcare tools will be described.

3.2. Risks of social computing applications in healthcare

The risks associated with the use of social computing applications for healthcare purposes include [5], [6], [13], [14], [16], [24], [25]:

- **Blogs:** There is a lack of reliability of the information provided in blogs which raises trust issues. Medical information provided in social computing platforms is prone to inaccuracy. Information quality is deemed the most important attribute for users of health information. According to [14] "The quality of the information on wikis, blogs and social networking sites is debatable".
- **Social games:** The use of social games for health education has been associated with risks for both mental and physical health. Constantly playing online games may lead to seizures and muscle injuries. Social isolation can also result from people playing social games so excessively that they disconnect from their physical environments.
- **Social networks:** Patient data provided in social networking sites can be misused by third-parties. This raises the issue of privacy and it remains a primary concern for the users of social computing. Another problem is that individuals can take the information provided by healthcare professionals out of context. This is because not everyone is health literate. Health literacy has been formally defined as the ability of an individual to read and understand prescription bottle labels, appointment slips, and other important health-related materials. Social computing requires individuals who use the platform for health reasons to be able to perform these tasks in order to fully reap the benefits of participating in their healthcare.
- **Social media:** People who create podcasts may only present information that is relevant or favourable to them, which promotes bias. This can mislead individuals who use this information.
- **Social knowledge sharing:** Wikis are prone to vandalism and hackers. This means that information can be changed or removed. The fact that information is provided anonymously on wikis raises concerns of the person's integrity and how factual the information they provide is.

The preceding sections described benefits and risks of using social computing applications for healthcare purposes. Table 1 summarises these risks and benefits.

Type	Benefits	Risks
Blogs	First-hand information Ease of use	Lack of reliability Trust issues Information inaccuracy
Social games	Educational awareness and learning Positive behavior change Motivational Improve wellbeing	Mental health problems Physical health problems
Social Networks	Psychological sense of community Fight social isolation	Misuse of patient information Privacy concerns Information used out of context
Social media	Support for medical professionals in remote areas Education and training	Misleading information

Social knowledge sharing	Quick update of new developments Resource sharing	Vandalism and hackers Information inaccuracy

Table 1: Risks and benefits of social computing applications that are used as a healthcare tool.

4. DISCUSSION

Social computing is a trend that has brought about change in the way that healthcare is being offered as it promotes information sharing, collaboration and so forth. Patients, and healthcare providers alike, are looking for new ways to increase patient knowledge and support self-management in order to improve healthcare outcomes. Combining healthcare tools and social computing applications creates new levels of patient participation in their own healthcare. Patients are connected with the healthcare providers as well as other health stakeholders participating in their healthcare.

As stated previously, blogs, social games, social networks, social media and social knowledge sharing tools are examples of social computing applications that can be used as healthcare tools. The benefits of these include promoting information exchange between patients and healthcare providers. Patients are empowered to take more ownership of their health and participate in decision-making. Education and training is also provided for medical professionals, which may make them more proficient in their field. Patients are also given health education training and awareness.

As much as there are these advantages, risks also exist. These relate to the quality of the information provided and also the well-being of the individuals, possible abuse of privacy, misunderstandings from the readers of information provided by healthcare providers, mental and health problems and also misinformation due to bias. The benefits of these social computing applications offer great opportunities for the health industry even in light of the risks.

5. CONCLUSION AND FUTURE WORK

The purpose of this paper was to highlight risks and benefits that come with the use of social computing applications as healthcare tools. Social computing was discussed, giving examples of the applications. The use of these applications as healthcare tools was described, as well as risks and benefits associated with employing social computing applications as healthcare tools. Future research includes finding ways to mitigate risks that particularly face social computing applications when they are used as healthcare tools.

ACKNOWLEDGEMENTS

The financial assistance of the South African National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

REFERENCES

[1] C. Coyle and H. Vaughn, "Social Networking: Communicatipn Revolution or Evolution," **Bell Labs Tech. J**., vol. 13, no. 2, 2014, pp. 12–17, doi: 10.1002/bltj.

[2] J. M. Mayer, R. P. Schuler, and Q. Jones, "Towards an understanding of social inference opportunities in social computing," **Proc. 17th ACM Int. Conf. Support. Gr. Work - Gr. '12**, 2012, p. 239, doi: 10.1145/2389176.2389212.

[3] I. King, J. Li, and K. T. Chan, "A brief survey of computational approaches in Social Computing," *2009* **Int. Jt. Conf. Neural Network*s***, 2009, pp. 1625–1632, doi: 10.1109/IJCNN.2009.5178967.

[4] F. Wang, D. Zeng, K. M. Carley, and W. Mao, "Social Computing : From Social Informatics," **IEEE Intell. Syst**., 2007, pp. 79–83, doi: 10.1109/MIS.2007.41.

[5] P. H. Keckley and M. Hoffmann, "Social Networks in Health Care: Cummunication, collaboration and insights," 2010.

[6] J. Sarasohn-Kahn, "The Wisdom of Patients: Health Care Meets Online Social Media," 2008.

[7] J. Williams, "Social Networking Applications in Health Care : Threats to the Privacy and Security of Health Information," **ICSE Work. Softw. Eng. Heal. Care**,2010,pp. 39–49, doi: 10.1145/1809085.1809091.

[8] M. N. K. Boulos and S. Wheeler, "The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education," **Heal. Inf. Libr. J**., vol. 24, no. 1, 2007, pp. 2–23, doi: 10.1111/j.1471-1842.2007.00701.x

[9] M. Tavakolifard and K. C. Almeroth, "On Some Challenges for Online Trust and Reputation Systems," Norwegian University of Science and Technology, 2012.

[10] A. Fu, "How to Get the Most Value from Social Computing for Business with Microsoft," 2008.

[11] R. K. F. IP and C. Wagner, "Weblogging: A study of social computing and its impact on organizations," **Decis. Support Syst**., vol. 45, no. 2, 2008, pp. 242–250, doi: 10.1016/j.dss.2007.02.004.

[12] W. Rafelsberger and A. Scharl, "Games with a purpose for social networking platforms," **Proc. 20th ACM Conf. Hypertext hypermedia HT 09**, 2009, p. 193, doi: 10.1145/1557914.1557948.

[13] M. Papastergiou, "Exploring the potential of computer and video games for health and physical education: A literature review," **Comput. Educ.**, vol. 53, no. 3, 2009,pp.603–622,doi: 0.1016/j.compedu..04.001.

[14] E. Randeree, "Exploring Technology Impacts of Healthcare 2.0 Initiatives," **Telemed. e-Health**, vol. 15, no. 3, 2009, pp. 255–261.

[15] L. Bos, A. Marsh, D. Carroll, S. Gupta, and M. Rees, "Patient 2 . 0 Empowerment," in **Proceedings of the 2008 International Conference on Semantic Web & Web Services SWWS08**, 2008, pp. 164–167.

[16] K. Ala-mutka, D. Broster, R. Cachia, C. Centeno, C. Feijóo, A. Haché, S. Kluzer, S. Lindmark, W. Lusoli, G. Misuraca, C. Pascu, Y. Punie, and J. A. Valverde, "The Impact of Social Computing on the EU Information Society and Economy The Impact of Social Computing on the EU Information Society and Economy," 2009.

[17] B. Dolan, "Mobile, social, fun: Games for Health," *Report*,2011.[Online].Available: http://mobihealthnews.com/15031/mobile-social-fun-games-for-health/. [Accessed: 30-Jul-2015].

[18] B. O'Hara, B. I. Fox, and B. Donahue, "Social media in pharmacy : Heeding its call , leveraging its power," 2013.

[19] B. W. Hesse, D. Hansen, T. Finholt, S. Munson, and J. C. Thomas, "Social Participation in Health 2.0," **Computer (Long. Beach. Calif*)***., vol. 43, no. 11, 2011, pp. 45–52, doi: 10.1109/MC.2010.326.Social.

[20] G. Hobgen, "Security Issues and Recommendations for Online Social Networks," no. 1, 2007.

[21] C. Cole, "Health 2.0 Risks to Providers," 2008. [Online]. Available: http://www.hcplive.com/medical-news/health_risks_to_providers. [Accessed: 29-Jul-2015].

[22] "Medical Ethics and Blogging: Think Before You Post," *Medical ethics and blogging*, 2007. [Online]. Available:http://www.hcplive.com/medical-news/medethics. [Accessed: 29-Jul-2015].

[23] C. G. Brown-johnson, B. Berrean, and J. K. Cataldo, "Development and usability evaluation of the mHealth Tool for Lung Cancer (mHealth TLC): A virtual world health game for lung cancer patients," **Patient Educ. Couns.**, vol. 98, no. 4, 2015, pp. 506–511, doi: 10.1016/j.pec.2014.12.006.

[24] G. Eysenbach, "Medicine 2.0: Social networking, collaboration, participation, apomediation, and openness," **J. Med. Internet Res.**, vol. 10, no. 3, 2008, pp. 1–14, doi: 10.2196/jmir.1030.

[25] J. E. W. C. van Gemert-Pijnen, **Improving eHealth**, Portland: Eleven international publishing, 2013.

CHAPTER SIXTEEN

PERSONAL HEALTH RECORDS IN THE SOUTH AFRICAN HEALTHCARE LANDSCAPE: A SWOT ANALYSIS

AVUYA MXOLI, NICKY MOSTERT-PHIPPS AND MARIANA GERBER

Introduction

The South African healthcare system is facing extensive financial difficulties when it comes to caring for patients with preventable lifestyle diseases (Watermeyer 2013). A large proportion of this consists of patients with hypertension and diabetes, constituting approximately 17 million visits to healthcare centers in South Africa each year. In an attempt to control this, the South African Department of Health has implemented a strategic plan to prevent and control non-communicable diseases. One of the strategies relates to increasing health awareness and healthy lifestyle promotion (Watermeyer 2013). South Africa is in the process of implementing the National Health Insurance (NHI), which will be offering more effective preventative care as opposed to the current South African healthcare system that is highly hospital-centric with a strong curative focus (Department of Health 2011).

A Personal Health Record (PHR) is an electronic web-based application that allows an individual to create and maintain his health information in one central place. It is evident that PHRs can aid in promoting health awareness and also assisting healthcare providers in the care process (The Markle Foundation 2004, Lehman et al. 2006, Sprague 2006). Even though there are documented benefits of PHR use, adoption rates are typically low, especially in developing countries (Dohan, Abouzahra, and Tan 2014).

Currently, there is little documentation on factors that can affect the adoption and meaningful use of PHRs in the South African context. This chapter will report on the results of a SWOT analysis and highlight the Strengths, Weaknesses, Opportunities and Threats related to PHRs in the South African context. The intent is that the results of the SWOT analysis might be used to strengthen and guide the adoption and meaningful use of PHRs in the South African context.

The next section will describe the concept of a Personal Health Record in more detail.

Personal Health Records

A Personal Health Record (PHR) is an electronic web-based record that is created, owned and maintained by an individual as a running record of his health history (Tang et al. 2006, Christopherson 2005, Sprague 2006). The information gathered in the PHR is a collation of the different health procedures they have undergone, allergies, past and present illnesses, immunizations, medication, test results and so forth (Tang et al. 2006). A PHR is especially beneficial to those patients managing chronic conditions like diabetes or hypertension and as well as those who suffer from life-threatening diseases such as cancer, HIV/AIDS or tuberculosis (The Markle Foundation 2004).

General benefits associated with the use of PHRs include the following (The Markle Foundation 2004, Tang et al. 2006):

- Empowering individuals and their families by:
    1. Providing them with useful information regarding their health problems to aid them in understanding and managing these.
    2. Allowing them to actively participate in their care-process and be part of decision-making.
    3. Helping them to monitor their health with regards to keeping track of blood pressure, glucose levels, noting symptoms as they occur, and so forth.
    4. Fostering a collaborative care plan between friends and family members of the patient.
    5. Providing individuals with means to set reminders and schedule important preventative services.

9. Cultivating a better relationship between the patient and healthcare provider by improving their communication and information sharing capabilities.
10. Improving the quality of care that patients receive by helping them provide a more comprehensive health history which will help the healthcare provider to better understand the patient's treatment plans and perform better diagnoses.
11. Improving the care process of patients with chronic conditions and thus yielding better outcomes.
12. Promoting earlier interventions when patients with chronic conditions encounter a problem or notice new symptoms.

Despite these benefits associated with PHRs, adoption rates are typically low, especially in developing countries.

SWOT Analysis

A Strength, Weakness, Opportunity, and Threats (SWOT) analysis provides a framework for identifying and analysing internal (Strength and Weaknesses) and external (Opportunities and Threats) factors that may have an impact on the viability and success of a project, product, individual or organization (TechTarget n.d.). The results of a SWOT analysis are typically presented in a 2x2 matrix and examine the elements indicated in Table 16-1 (TechTarget n.d.).

	Helpful	**Harmful**
Internal Origin	**STRENGTHS** Internal factors that support a successful outcome.	**WEAKNESSES** Internal factors that hinder a successful outcome.
External Origin	**OPPORTUNITIES** External factors that may contribute to a beneficial outcome.	**THREATS** External factors that may constrain a beneficial outcome.

Table 16-1. SWOT analysis (TechTarget n.d.)

This chapter reports on the results of a SWOT analysis that was done in order to identify factors that influence the adoption and meaningful use of PHRs in the South African context. The SWOT analysis was completed in two phases.

Phase 1 of the analysis focused on the internal factors (Strengths and Weaknesses) related to PHRs. Data collection and analysis for this phase focused on factors related to the concept and nature of a PHR to identify strengths and weaknesses that may influence the adoption and meaningful use of PHRs in the South African context.

Phase 2 focused on the external factors (Opportunities and Threats). Data collection and analysis for this phase focused on the following aspects:

- Since a PHR is typically owned, created, and managed by an individual, the influence of consumers on the adoption and meaningful use of PHRs were considered. Only two recorded studies that focus on South African consumers' perceptions towards PHRs could be identified by the authors. In 2012 a survey was conducted in the Nelson Mandela Bay (NMB) area of South Africa that investigated the perceptions of consumers regarding PHRs (Pottas and Mostert-Phipps 2013). A similar nation-wide survey was conducted in 2013 (Jojo and Mostert-Phipps 2013).
- PHRs are typically web-based and as such technical factors such as Internet access, Internet literacy levels and so forth were considered.
- PHRs have far-reaching implications for healthcare providers and the greater healthcare system and as such factors related to these aspects in the South African context were also considered.

The following section indicates the results of the SWOT analysis.

Results

Table 16-2 indicates the Strengths, Weaknesses, Opportunities and Threats as identified through the SWOT analysis described in the previous section. Each of these identified factors is described in detail in the discussion section that follows.

	Helpful	Harmful
Internal Origin	**STRENGTHS** • Protection of sensitive patient information • Reduction of information loss • Improvement of the quality of the recorded information • Improvement of provider interactions • Accessibility to information • Bigger cost savings • Increased patient safety	**WEAKNESSES** 1.Data inaccuracy 2.Privacy and security 3.Digital divide 4.Trust 5.Interoperability limitations 6.Low health literacy 7.Deliberate omission of information **8.**Legal issues
External Origin	**OPPORTUNITIES** • Importance of medical history knowledge • Benefits offered by PHRs • Personal record keeping practices • Willingness to pay for PHR use • Improved communication with healthcare providers • Improved understanding of own health • Improved sense of control • Access to mobile technology • National Health Insurance (NHI) • Managing and reducing costs • Improved quality of healthcare	**THREATS** • Lack of awareness • Personal record keeping practices • Internet access • Internet literacy • Privacy concerns

Table 16-2. Results of SWOT analysis

Discussion

Strengths

There are various factors related to the nature of PHRs that support the adoption and meaningful use of PHRs (Endsley et al. 2006, Tang et al. 2006, Noraziani et al. 2013, Miller and Sim 2004, Kahn, Aulakh, and Bosworth 2009, Archer et al. 2011, Zieth et al. 2014):

- **Protection of sensitive patient information:** An individual's health information contains parts that should be kept private. This privacy is not safeguarded adequately with the use of paper-based health records; therefore a web-based PHR that has security measures can achieve this.
- **Reduction of information loss:** PHR data is safe from getting lost or damaged due to natural disasters such as fires or hurricanes. Information stored on paper is also at a risk of becoming defragmented and thus hard to find.
- **Improvement of provider interactions:** Information stored in a PHR can be accessed by different healthcare providers if the patient grants them access. This assists in giving a more comprehensive history of the patient's health information which will aid in better continuity of care.
- **Accessibility to information:** Patients can grant healthcare providers access to their health information even in emergency situations. Healthcare providers can also send their notes to patients easily and quickly instead of the patient having to go physically to get authorization to access their paper records. This also frees healthcare providers from being limited to face-to-face interactions with the patient.
- **Improvement of the quality of the recorded information:** Doctors' handwriting sometimes is not clear for other people to understand. Having to enter data by typing reduces the chances of having misunderstandings.
- **Increased patient safety:** Providing drug-interaction checks for patients and healthcare providers which would alert them of possible contraindications, side effects and allergic reactions. Patients and healthcare providers can also be made aware of missed procedures and any lapses in adherence to treatment regimes.

- **Bigger cost savings:** A PHR has the potential to reduce clinical errors and duplication of tests and procedures. This can save the patient some money.

Weaknesses

Unfortunately the way that PHRs are designed introduces some barriers to adoption and meaningful use as well. These barriers will be discussed below (Tang et al. 2006, Endsley et al. 2006, Miller and Sim 2004, Kahn, Aulakh, and Bosworth 2009, Archer et al. 2011, Noraziani et al. 2013, Lober et al. 2006, Witry et al. 2010):

- **Data inaccuracy:** Allowing patients to not only view, but to enter their own data into the PHR may lead to issues of data inaccuracy because they use their own discretion and probably do not have a medical background.
- **Privacy and security:** Individuals using PHRs may worry about the safety of their health information because PHRs are hosted on the Internet.
- **Digital divide:** PHRs use computers and not everyone has a technical background. This does not only apply to patients. Other stakeholders may also need some training in order to efficiently use PHRs. Some people may even experience problems accessing their PHRs because of environmental issues such as poor Internet connection. People with cognitive impairments or the elderly, may also find it difficult to use a PHR.
- **Trust:** Some healthcare providers may feel threatened by the fact that patients will have this much control of their health information. They may not trust patients enough to be able to manage their PHRs on their own and thus not trust what is contained therein.
- **Interoperability limitations:** Not all health information systems may be interoperable with the patient's PHR and thus it may be difficult to share and exchange data.
- **Low health literacy:** Healthcare providers are concerned that patients might overreact when they come across some medical terms that have been entered by the doctors because they do not use layman's vocabulary on the health record.
- **Deliberate omission of information:** A PHR is owned by the patient who can decide what is captured. Some doctors have voiced concern that a patient might not state everything about their health status in the PHR because of possible insurance complications.

- **Legal issues:** Healthcare providers are wary of the possibility of being accused of negligence because they rely on the data that is in the PHR, provided by the patient, to make crucial decisions about their care.

Opportunities

The following external factors may contribute to the adoption and meaningful use of PHRs in South Africa (Jojo and Mostert-Phipps 2013, Valter 2013, Pottas and Mostert-Phipps 2013, Statistics South Africa 2013, Sprague 2006, Department of Health 2011, The Markle Foundation 2004, Lehman et al. 2006):

- **Importance of medical history knowledge:** Whilst 42% of the participants in the national survey indicated that their healthcare provider was not informed of their full medical history, 70% of the participants indicated that it is extremely important for their healthcare provider to be aware of their full medical history.
- **Benefits offered by PHRs:** Once they were made aware of the existence of PHRs, participants in the national survey expressed great interest in the features of web-based PHRs, especially viewing their medical records, test results and educational materials related to their health, as well managing medication lists, setting reminders for preventative health services and communicating with their healthcare providers. About 69% of the participants indicated that they are interested in making use of PHRs to view their health information and manage their healthcare.
- **Personal record keeping practices:** The study conducted in the NMB area indicated that it was more likely for participants with chronic medical conditions to keep a record of their medical history. Although this currently often takes a paper-based format it does indicate that a PHR could prove beneficial to individuals suffering from chronic conditions.
- **Willingness to pay for PHR use:** As seen in Figure 16-1, it was encouraging to note that a large number of participants in the national survey expressed a willingness to pay a monthly fee for the use of a PHR.

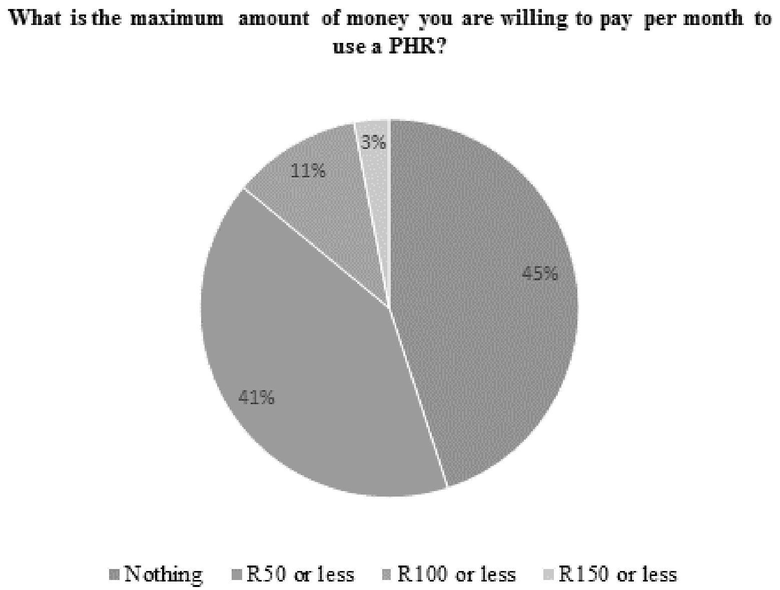


Figure 16-1. Willingness to pay for PHR use (Jojo and Mostert-Phipps 2013).

- **Improved communication with healthcare providers**: Participants in the national survey indicated that PHRs could potentially improve communication between themselves and their healthcare providers, with 48% of the participants envisioning a possible great improvement.
- **Improved understanding of own health:** The majority (53%) of the participants in the national survey indicated that they believe that PHRs could greatly improve their understanding of matters related to their own health.
- **Improved sense of control:** 53% of the participants in the national survey indicated that PHRs could greatly improve their sense of control over their own healthcare.
- **Access to mobile technology:** Statistics South Africa's General Household Survey for 2013 revealed that at least 81.9% of South African households had access to at least one cellular phone. Mobile technology has made access to the Internet much more accessible to South African households with 30.8% of households having mobile access to the Internet.

- **National Health Insurance (NHI):** One of the objectives of the planned National Health Insurance (NHI) in South Africa is to re-engineer primary healthcare services to focus mainly on health promotion and preventative care. PHRs can enable individuals to better manage their healthcare and thus play a significant role in preventative care. PHRs could be utilized to better educate patients about their medical conditions, improve adherence to medical and lifestyle changes, and engage them in medical decision-making. Its role in increasing health awareness could prove invaluable in promoting health and supporting healthcare providers in offering more effective preventative care as opposed to the South African healthcare system that is currently highly hospital-centric with a strong curative focus.
- **Managing and reducing costs:** The use of PHRs may reduce healthcare costs due to fewer admissions and emergency room visits, avoidable drug-drug interactions, avoidable over-use of medications and increased use of over-the-counter medication in treating common chronic conditions. This benefit could ensure support from healthcare funders for the adoption and use of PHRs.
- **Improved quality of healthcare:** Participants in the national survey mentioned previously indicated that PHRs have the potential to improve the healthcare that they receive, with 45% envisioning a potential great improvement and 33% a slight improvement. Participants also indicated that PHRs can contribute to a reduction in medical errors due to a lack of information, with 37% indicating a potential great improvement and 38% a slight improvement.

Threats

There are also external factors that threaten the adoption of PHRs and hence lower willingness and ability to use them. Below are some of these factors (Pottas and Mostert-Phipps 2013, Statistics South Africa 2013):

- **Personal record keeping practices:** The study conducted in the NMB area indicated that most participants (69%) did not keep a record of their full medical history. Those participants that did keep a record of their medical history primarily made use of paper-based means.

- **Lack of awareness:** 84% of participants in the NMB survey indicated that they were not aware of the existence of PHRs before participating in the survey.
- **Internet access:** Statistics from Statistics South Africa's General Household Survey for 2013 reveal that access to the Internet remains a problem in South Africa. As seen in Table 16-3, on average only 10% of South African households have access to the Internet at home. When considering access to the Internet outside the home, the statistics further revealed that for 16.1% of households at least one member of the household has access to the Internet at home and 9.6% at Internet cafes or educational facilities. These statistics exclude access to the Internet via mobile devices such as cellular phones or 3G cards.

Place Internet is accessed	**RSA**
At home	10%
At work	16,1%
Using mobile devices	30,8%
At Internet cafes or educational facilities	9,6%

Table 16-3. SA Household Internet access by place of access (Statistics South Africa 2013).

- **Internet literacy:** The national survey referred to in previous sections indicated that participants in that survey did not rate themselves as particularly Internet literate. When asked to rate their Internet literacy level, less than half of the participants considered themselves to be 'skilled' or 'very skilled' in terms of navigating the Internet to search for information (45%) and uploading and downloading information (47%). Slightly more participants (52%) rated themselves as 'skilled' or 'very skilled' in terms of their ability to send e-mails.
- **Privacy concerns:** In the NMB survey mentioned previously, the majority of participants (58%) indicated that they would be concerned about the privacy of their personal health information when using a PHR.

Conclusion

This chapter reports on the results of a SWOT analysis that was completed in order to identify factors that influence the adoption and meaningful use of PHRs in the South African context. Strengths and Weaknesses were identified through a literature review focusing on studies that describe the nature of benefits and drawbacks associated with web-based PHRs. Opportunities and Threats were identified through a literature review that focused specifically on the South African context. The results presented and discussed in this chapter can be used to strengthen and guide the adoption and meaningful use of PHRs in the South African context. It is encouraging to note that there are various Strengths and Opportunities that can be explored to encourage the adoption of PHRs by South African consumers.

Acknowledgements

The financial assistance of the South African National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

Archer, N., Fevrier-Thomas, U., Lokker C., McKibbon, K.A., and Straus, S.E. (2011). Personal Health Records: A Scoping Review. *Journal of the American Medical Informatics Association,* 18(4): 515–22. doi:10.1136/amiajnl-2011-000105.

Christopherson, Gary A. (2005). HealthePeople: Person-Centered, Outcomes-Driven, Virtual Health Systems. In: Person-Centered Health Records: Toward HealthePeople, edited by James E. Demetriades, Robert M. Kolodner, and Gary A. Christopherson: 21-39. Springer.

Department of Health. (2011). National Health Insurance in South Africa. Vol. 59. doi:10.1111/1536-7150.00099.

Dohan, Michael S., Abouzahra, Mohamed, and Tan, Joseph. (2014). Mobile Personal Health Records: Research Agenda for Applications in Global Health. In 2014 47th Hawaii International Conference on System Sciences: 2576–2585. Waikoloa: Ieee. doi:10.1109/HICSS.2014.325. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6758925.

Endsley, Scott, Kibbe, David C, Linares, Anthony, and Colorafi, Karen. (2006). An Introduction to Personal Health Records. *Family Practice Management*, 13(5): 57–62.

Jojo, Sinelizwi, and Mostert-Phipps, Nicky. (2013). Awareness and Interest in Web-based Personal Health Records. In Proceedings of the 15th Annual Conference on World Wide Web Applications. Cape Town: Cape Peninsula University of Technology.

Kahn, James S., Aulakh, Veenu, and Bosworth, Adam. (2009). What It Takes: Characteristics of the Ideal Personal Health Record. *Health Affairs,* 28(2): 369–76. doi:10.1377/hlthaff.28.2.369.

Lehman, H.P., Abbott, P. A., Roderer, N. K., Rothschild, A., Mandell, S., Ferrer, J.A., et al. (2006). Aspects of Electronic Health Records (2nd ed.). Springer.

Lober, W.B., Zierler, B., Herbaugh, A., Shinstrom, S.E., Stolyar, A., Kim, E.H., and Kim, Y. (2006). Barriers to the Use of a Personal Health Record by an Elderly Population. AMIA Annual Symposium Proceedings. AMIA Symposium: 514–18.

Miller, Robert H., and Sim, Ida. (2004). Physicians' Use of Electronic Medical Records: Barriers and Solutions. *Health Affairs*, 23(2): 116–126. doi:10.1377/hlthaff.23.2.116.

Noraziani, K., Nurul'Ain, A., Azhim, M.Z., Eslami, S.E., Drak, B., Sharifa Ezat, W.P., and Akma, S.N. (2013). An Overview of Electronic Medical Record Implementation in Healthcare System: Lesson to Learn. *World Applied Sciences Journal*, 25(2): 323–32. doi:10.5829/idosi.wasj.2013.25.02.2537.

Pottas, Dalenca, and Mostert-Phipps, Nicky. (2013). Citizens and Personal Health Records - the Case of Nelson Mandela Bay. *Studies in Health Technology and Informatics*, 192: 501–4. http://www.ncbi.nlm.nih.gov/pubmed/23920605.

Sprague, Lisa. (2006). Personal Health Records: The People's Choice? NHPF Issue Brief / National Health Policy Forum, George Washington University, no. 820: 1–13. doi:17146910.

Statistics South Africa. (2013). General Household Survey 2013. Pretoria. http://beta2.statssa.gov.za/publications/P0318/P03182013.pdf.

Tang, Paul C., Ash, Joan S., Bates, David W., Overhage, Marc J., and Sands, Daniel Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association*, 13(2): 121–27. doi:10.1197/jamia.M2025.records.

TechTarget. (n.d.). 'What is SWOT analysis (strengths, weaknesses, opportunities and threats analysis)? - Definition from WhatIs.com'. Last accessed May 09 2015 http://searchcio.techtarget.com/definition/SWOT-analysis-strengths-weaknesses-opportunities-and-threats-analysis.

The Markle Foundation. (2004). Connecting Americans to their Healthcare Final Report. Last accessed June 26 2014. http://www.policyarchive.org/collections/markle/index?section=5&id=15525

Watermeyer, Laura. (2013). 'Government unveils NCD strategic plan'. Last accessed June 27 2014. http://www.health-e.org.za/2013/09/18/government-unveils-ncd-strategic-plan/.

Witry, Matthew J., Doucette, William R., Daly, Jeanette M., Levy, Barcey T., and Chrischilles, Elizabeth A. (2010). Family Physician Perceptions of Personal Health Records. Perspectives in Health Information Management / AHIMA, American Health Information Management Association 7 (January): 1d. http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2805556&tool=pmcentrez&rendertype=abstract.

Zieth, Caroline R., Chia, Lichun R., Roberts, Mark S., Fischer, Gary S., Clark, Sunday, Weimer, Melissa, and Hess, Rachel. (2014). The Evolution, Use, and Effects of Integrated Personal Health Records: A Narrative Review. *Electronic Journal of Health Informatics,* 8(2).

Personal Health Records: Design considerations for the South African context

A. Mxoli
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
Council for Scientific and Innovation Research, Pretoria, South Africa
amxoli@csir.co.za
N. Mostert-Phipps
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
nicky.mostert-phipps@nmmu.ac.za
M. Gerber
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
mariana.gerber@nmmu.ac.za

Abstract:
A Personal Health Record (PHR) is a set of internet-based tools that allow individuals to create, store and coordinate their lifelong health information in one place making it available to relevant parties. It typically contains the individual's demographic information, medical care providers' details, health summary, family history, list of past and current illnesses, symptoms, allergies, medication and so forth. A PHR introduces many advantages as far as improving the health status of people. These include better doctor-patient relationships, improved health knowledge, better monitoring of chronic illnesses and many others. The South African health system is in need of a more preventative approach to healthcare as opposed to its current system that is considered as a highly curative. South Africa's planned National Health Insurance (NHI) aims at achieving this. The South African Department of Health also aims at improving access to quality health care, increasing patients' participation and the dignity afforded to them, reducing underlying causes of illnesses, injury, and disability, to mention a few. A PHR can prove useful to achieve these health goals and more in South Africa.

There is, however, no PHR that is specifically aimed at the South African population and thus adoption rates in South Africa are typically low. There is also a lack of design guidelines for PHRs that are suitable for the needs of South African consumers. This paper highlights

design guidelines and other factors that should be considered when developing a PHR for use in the South African context. Guidelines related to the interoperability, comprehensiveness, legal value, and availability of PHRs are discussed.
Keywords:
Personal Health Record, South Africa, Design guidelines

1. Introduction

South Africa as a developing country is faced with many challenges, quality healthcare provision being one of them. The country is faced with a burden of disease which deteriorates the quality of healthcare. A Lancet report terms this as the quadruple burden of disease which consists of (Department of Health 2011):

- HIV/AIDS and TB;
- Maternal, infant and child mortality;
- Non-communicable diseases; and
- Injury and violence.

These demand a preventative approach to healthcare provision rather than the current health system of South Africa which is considered highly curative (Department of Health 2011). According to the National Health Act (2004), the people of South Africa using health services have the right to participate in decisions that affect their personal health and treatment. It is recommended that the National Department of Health's e-Health infrastructure should focus on person-centric healthcare (Department of Health & CSIR 2014). There is a National e-Heath strategy (2012) that, amongst other principles, focuses on patient-centeredness. This means providing care that focuses on respecting and being responsive to individual patient needs and values and also making sure that these guide all clinical decisions regarding the patient's health. This necessitates a solution that promotes the health goals of South Africa and a Personal Health Record (PHR) may be suitable for this.

A PHR gives individuals direct access to the health information as it allows them to create, manage and share their health information in one central place (The Markle Foundation 2003). They decide which parts to make available for other parties to see and this feature becomes useful when a doctor is involved in the monitoring of one's health status. Family members can also participate in the health management of an individual that owns a PHR and this increases the involvement and promotes better care (Archer et al., 2011:515). PHRs introduce many benefits and these include but are not limited to the following (Kim & Johnson 2002; Tang et al. 2006; The Markle Foundation 2004):

- **Improved patient and doctor communication:** PHRs allow doctors and patients to communicate beyond the usual face-to-face encounters. This fosters a better relationship and better understanding between the two parties.
- **Better health information knowledge:** There are PHRs that provide individuals with health information to educate them about what is currently happening in the world of medicine.
- **Improved quality of care:** Individuals who use PHRs can take to their doctors a comprehensive health summary which contains past procedures that had already been conducted on the patient. This avoids duplication and speeds up the diagnosis process.
- **Increased patient safety:** Some PHRs provide individuals with information about possible drug interactions, side effects, allergic reactions and so forth.
- **Better family support:** There are PHRs that allow for family members to be involved in taking care of an individual's health granting them access to the PHR.

Despite these benefits of PHRs, adoption rates in South Africa are significantly low. A survey conducted in the Nelson Mandela Bay area of South Africa in 2012 indicated that 84% of participants were not aware of the existence of PHRs (Pottas & Mostert-Phipps 2012). It is vital to understand the types of individuals and consumers of PHRs and the functions they mostly use in order to create PHRs that will actually benefit them (Tang et al. 2006). There is no PHR system that has been developed specifically for the South African population.

This paper will highlight design considerations and other factors that should be considered when developing a PHR that will benefit South Africans. A literature review focusing on content relevant to the South African context was employed to gather data related to factors that should be considered when developing a PHR for the South African market.

2. Design considerations for a South African PHR

This section will highlight some design considerations that should be considered when developing a PHR for the South African market. A PHR is a lifelong health record that has been gathered from different sources at different time intervals. It is crucial that the information contained in such a record has some qualities that will ensure its usefulness in decision-making for a patient's health. There are four core characteristics of lifelong health records as identified by Van der Westhuizen and Pottas (2010) that should be considered when designing a PHR. These are interoperability,comprehensiveness, legal value and availability. The subsections below elaborate on these charactertistics and design associations related to them.

2.1 Interoperability

Interoperability refers to the ability of information and communication technology (ICT) systems as well as the business processes they support, to communicate through the sharing and exchange of information and knowledge (IDABC 2004). This allows for a greater two-way communication of the patient's health data. PHRs are managed and owned by the patient. He can decide if he wants to share the content of his PHR with his healthcare provider or not and that also depends if that particular PHR has that feature. This, however, limits the chances of better coordination and continuity of care as the data stored in the PHR may only be recorded by the patient. There are other health systems in place that contain patient health information but are not owned by the patient.

An Electronic Medical Record (EMR) contains medical information and treatment history of a patient gathered in one practice while an Electronic Health Record (EHR) contains data collected from more than one practice (Garrett & Seidman 2011). An EHR is a patient's medical record collected from various health organizations. It may include data such as patient demographics, test results, images, symptoms and so forth. This data may be gathered from various stakeholders such as the patient's primary healthcare provider, specialist, pharmacists, nurses etc. (Ludwick & Doucette 2009). Everyone involved in the patient care can have access to the EHR, including the patient (Caligtan & Dykes 2011). A patient can upload information from their PHR to the EHR and vice versa (Mostert-Phipps 2012). This improves the quality of data in that the patient's health record is more comprehensive, containing all relevant information from the various sources which aids in better decision-making (Caligtan & Dykes 2011; Hargreaves 2010).

Interoperability between health systems such as EMRs, EHRs and PHRs is critical in a national healthcare system (Department of Health & CSIR 2014). South Africa, according to the eHealth Strategy South Africa (2012), is planning on implementing a National Health Insurance (NHI) and this is dependent on an effective national electronic, patient-based information system. South African health information systems have, however, been faced with some challenges namely: fragmentation and lack of coordination, too many manual systems and where automation existed, a lack of interoperability was a problem (NDoH 2012).

The question always rises with regards to how PHR applications can interact with EHRs (Kharrazi et al. 2012). The lack of interoperability between various systems is a major obstacle to realizing the potential benefits of eHealth (Department of Health & CSIR 2014). Amongst others, the eHealth strategy of South Africa (2012) has principles that address this problem.

One of the principles is to enable integration between systems wherever appropriate. One of the ways they aim to achieve this is through the establishment of common data standards and terminology across information systems. The document has objectives for the e-Health interventions that are required and these include eHealth standards. Establishing a national standards authority, facilitating training in eHealth standards and finally localizing eHealth interoperability standards and mandating their use all form part of the objectives. The eHealth strategy has priorities and strategic priority three is standards and interoperability, this highlights the importance of interoperability between the country's health systems.

This need for interoperability has led to the development of a National Health Normative Standards Framework for eHealth in South Africa (HNSF). Its primary objective is to set the foundational basis for interoperability (Department of Health & CSIR 2014)

Using standards to govern the development of IT systems yields great advantages such as alignment, integration, flexibility, reusability, portability and reduced time to market (Department of Health & CSIR 2014). The implementation of proper standards is critical to the successful integration of PHRs with systems such as EHRs and EMRs. This can be achieved through the use of standardized messaging structures, medical vocabularies, comparable information, comparable terminology and agreed-upon means of communication, amongst others (Kharrazi et al. 2012; van Heerden, Tomlinson & Swartz 2012).

2.2 Comprehensiveness

For a health record to be useful, it should be comprehensive. This means the data entered in it must come from trusted parties, it must be up-to-date, correspond to real world objects, and it must be complete i.e. contain the entire health history (van der Westhuizen & Pottas 2010). There are standards that should be followed in order to ensure that the information contained in a PHR is comprehensive. The ISO multi-part standard on health informatics for the patient healthcard data includes the following standards that can be used to ensure comprehensiveness of a PHR (Department of Health & CSIR 2014; International Organization for Standardization 2004):

- **ISO 21549-1:2004(General Structure):** This standard defines the general structure of data that is contained in a PHR.
- **ISO 21549-2:2004(Common Objects):** It specifies a common framework for the content and basic structure of common objects used to construct PHR data. It does not define the specific data-sets for storage on devices.
- **ISO 21549-3:2004(Limited Clinical Data):** This provides the basic structure of data contained within the limited clinical data object. It does not specify the particular data sets for storage on devices.
- **ISO 21549-4:2004(Extended Clinical Data):** Specifies the basic structure of the data contained in the extended clinical data object. It is only applicable to situations where such data are recorded on, or transported by patient healthcare data cards
- **ISO 21549-5:2004(Identification Data):** Provides a common framework for the content and the structure of identification data held on healthcare data cards. It gives the specification for the basic structure of the data, without specifying the particular data-sets for storage on devices.
- **ISO 21549-6:2004(Administrative Data):** Specification of the basic structure of the data held within the administrative data object, without specifying the particular data-sets for storage on devices.

- **ISO 21549-7:2004(Medication Data):** Specification of the basic structure of the data held within the medication data object, without specifying the particular data-sets for storage on devices.
- **ISO 21549-8:2004(Links):** It defines a way to facilitate access to distributed patient records and/or administrative information using the PHR through references to individual patients' records and their subcomponents. The standard does not cover services relating to access control mechanisms, data protection mechanisms, access methods and other security services.

2.3 Legal Value

This characteristic speaks to the fact that the patient should have a way to grant/revoke access to his PHR. Only authorized parties should have access and be able to make changes to the PHR and there should be audit logs to monitor who had access to the PHR (van der Westhuizen & Pottas 2010). The most commonly recognized PHR adoption barriers are privacy and confidentiality concerns (Wynia & Dunn 2010). A study conducted in the Nelson Mandela Bay in South Africa by Jojo and Mostert-Phipps (2013) however, reveals that 70% of the participants are willing to share their PHR information with their primary care doctors, 52% with family members or friends and 48% with other healthcare providers. Participants were less inclined to share their health data with their employer (3%) and government officials (2%). This suggests that they are willing to have some parties access their PHRs but there is the concern of unauthorized parties gaining access too. A similar study was conducted in the Nelson Mandela Bay municipal area to gain insight on the attitudes of the citizens towards PHRs (Pottas & Mostert-Phipps 2012). It was found that 58% of the participants were concerned about their privacy when using a PHR.

In order to protect the PHR, some safeguards need to be implemented and these can be categorized as administrative, technical and physical safeguards (Maglogiannis 2011).

- **Administrative safeguards:** These address the security management process, assigned security responsibility, security aware and training and contingency planning.
- **Technical safeguards:** Access controls, audit controls, integrity and person or entity authentication and transmission security.

- **Physical safeguards:** These include facility access control, secure installation environment protection of devices and media controls.

Since the PHR is in full control of the individual, they play a huge role in ensuring their privacy. PHR users should therefore choose wisely when deciding on a PHR provider. They can also apply encryption methods to protect their data before handing it over to the provider which will be responsible for storing it (Li et al. 2013). According to Tang and Lansky (2005), a strong national leadership also plays a huge role in ensuring that the legislative and regulatory policies to protect the PHRs privacy and confidentiality are in place.

2.4 Availability

It is important that a PHR is available when a healthcare provider needs it. Failure of the PHR is not acceptable because once that happens, lives are put at risk. A health record should be continuously available for it to be deemed lifelong (van der Westhuizen & Pottas 2010). A PHR, therefore, should be made available at all times and should be easily accessible. This subsection will introduce some options that can make this possible.

South Africans that have access to the Internet at home are only 10% according to Statistics South Africa’s General Household Survey (2013). 9.6 % of the population accesses the Internet at Internet cafes or at educational facilities while 16.1 % access the Internet at work (Statistics South Africa 2013). This shows that South Africans have little access to the Internet. Looking at households that only use cellphones for their telecommunications, Statistics South Africa’s General Household Survey (2013), shows that they cover 81.9 %. This accounts for the high Internet access via mobile phones which is 30.8% (Statistics South Africa 2013).

Patients are increasingly searching for means to access their health records that are more accessible and portable (Archer et al. 2011; Maloney & Wright 2010. This creates the opportunity to utilize mobile PHRs (mPHRs) in order to better manage the health of the South African population. MPHRs are mobile applications that enable an individual to record, manage and store their health data (Dohan & Tan 2014). One can record symptoms, allergies, medications, access emergency information and so forth depending on the features offered by the mPHR they are using (Dohan & Tan 2014). They can also decide if they want to share this with others e.g. doctors or family members. The use of mPHRs in a diabetes case study has proven them to be successful as the participants could better manage their health (Preuveneers & Berbers 2008). People already access sensitive information via their cellphones such as cellphone banking, shopping, and maintaining their financial data. It is therefore highly likely that they will be comfortable with using mPHRs (Kharrazi et al. 2012).

Cellphones offer a sense of mobility as well as instant accessibility. This means a person will have access to his medical data anywhere and anytime he needs it. According to Kharrazi et al (2012), having instant access to one's PHR can significantly decrease errors and time needed to repeat health history, the need to recall past immunizations and medication history. Cellphones also come with features such as a camera, Global Positioning Systems (GPS), and touch-screen. These can prove to be useful to an mPHR because the camera can be used to scan and import documents, take pictures to describe symptoms, take video notes, or scan medication barcodes. The GPS may be used to locate healthcare providers nearby. Touch-screen interfaces can provide better data entry and navigation mechanisms hence improving usability (Kharrazi et al. 2012). The advancement in technology allows for the creation of new applications that can be applied to healthcare. South Africa is said to have the most advanced mobile phone and Internet industries in Africa therefore, mPHRs can prove useful in the eradication of poor health management in the country.

Using the mobile phone to access health applications demands infrastructure such as storage, processing power and bandwidth and this creates the need to make use of Cloud Computing (CC) capabilities (Dinh et al. 2013; Dohan & Tan 2014). CC can be defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance 2011). NIST describes the following major characteristics of CC (Mell & Grance 2011):

- **Ubiquitous network access**: resources are made available over the network through standard mechanisms that can be accessed over different platforms (e.g. smartphones).
- **On-demand self-service**: a user can have access to computing capabilities as needed without interacting with the service provider.

- **Resource pooling**: computing resources are pooled to help multiple users through a multi-tenant environment. The users share physical and virtual resources dynamically and these are assigned and reassigned as the users demand them.
- **Rapid elasticity**: this is the ability to dynamically scale the resources according to the user' demand.
- **Measured service**: a pay-per-use method is used to automatically control and optimize resource usage. This allows for resource usage to be monitored, controlled and reported, which promotes transparency between the service provider and user.

Using CC to access mPHRs means mobile devices will not require a powerful configuration such as CPU speed and memory because all the computing modules have been transferred to the Cloud (Dinh et al. 2013). Some of the advantages of using CC with the mobile phone also include extended battery life, and improved reliability. MPHRs used in conjunction with CC will provide pervasive access to Cloud-based health services thus promoting self and domestic care. This in turn will blur the boundaries that currently exist between the physical and digital worlds, allowing personalized and universal healthcare services (Sultan 2014).
Apart from interoperability standards, CC is another important cornerstone needed to streamline healthcare for maintaining health records, monitoring patients, managing diseases and care more efficiently and effectively (Zhang & Liu 2010). Healthcare providers are looking for more innovative and cost-effective means to address many of the problems facing healthcare (Sultan 2014). Cloud Computing has the potential to address some of these problems.

It can reduce healthcare integration costs, optimize resources and introduce a new era of innovations (Ahuja, Mani & Zambrano 2012). There is a great potential in CC for managing EHR/PHR systems in the US (Alagoz et al., 2010). CC can play a vital role in ensuring interoperability between disparate systems such as EMRs, EHRs and mPHRs. The fact that CC services can be accessed on any device ensures that these systems can communicate together. This feature is something healthcare IT is desperately in need of (Ahuja, Mani & Zambrano 2012). Data stored on a Cloud-based system would eliminate the need for an EHR to communicate with a PHR if a Cloud service can act as a storage mechanism and intermediary for data transfer between these health systems. This may also eliminate the problem with platform-specific software as well as incompatibilities between different operating systems used by different manufacturers (Kharrazi et al. 2012). CC is offered in three service models (Mell & Grance 2011; Gong et al. 2010):

- **Software as a Service (SaaS)**: The software or applications that users use are provided to them via the Internet on a pay-per-use basis instead of them incurring costs of downloading and maintaining software on the computers.
- **Platform as a Service**: The user has the ability to deploy applications they have acquired or created using a programming language that is supported by their vendor.
- **Infrastructure as a Service**: Infrastructure providers are able to deliver huge computing resources such as storage, network and processing power.

The ability for accessing a PHR on different platforms such as a mobile phone is supported by the SaaS model. This type of service would also be marketed to small practices that are looking to adopt EMR usage (Schweitzer 2014). The ability for patients to provide access to their health history and other information from their PHR stored in the cloud to hospitals is also made possible through the use of SaaS (Bahga & Madisetti 2013). EMRs built with the PaaS model could be offered to practices large enough to have their own IT support and are interested in rapidly customizing their EMR (Moore 2009). PaaS systems could also supply the software developers with the tools needed to add on the basic functionality that comes with an EMR. This would address the clinicians' concerns about EMR applications' agility and adaptability to local business workflow (Schweitzer 2014)

In terms of mPHR integration with EMRs, IaaS can be used in order to transfer the resources needed to support these healthcare systems. The costs of building and maintaining infrastructure will decrease while allowing better access to health information (Dohan & Tan 2014).

Cloud services are deployed according to different deployment models (Kuo 2011; Mell & Grance 2011; Zhang & Liu 2010):

- **Public cloud:** Cloud Computing resources are made available to the general public on a pay-per-use basis via the Internet. This Cloud is owned by the Cloud provider.
- **Private cloud:** This is operated exclusively for a particular organization e.g. healthcare facility. It is managed by that organization or by a third party.

- **Community cloud:** Cloud services are shared by a community of organizations that share a common goal e.g. healthcare facilities that want to share their EMRs. This is managed by the organizations or outsourced.
- **Hybrid cloud:** This is a combination of two or more cloud models (public, private or community). An organization may decide to manage some resources internally while outsourcing others.

Depending on the deployment model that an organization chooses, there are security issues that they should consider. Healthcare facilities, for instance, should decide whether they want to use private or public clouds. They should look at regulations that govern access to healthcare systems and how they can ensure the privacy and security of patient data (Dohan & Tan 2014). An in-depth understanding of the healthcare security and privacy concerns could be the first step towards the adoption of CC for healthcare systems (Zhang & Liu 2010). Once the challenges of CC have all been addressed, it seems that Cloud-based systems will likely become the norm in healthcare (Ahuja, Mani & Zambrano 2012).

3. Discussion

Health plays an important role in a country's well-being and should be treated as such. There are Health Information Technologies available that can play a supporting role in improving improve healthcare services such as EMRs, EHRs and PHRs. The challenge with these systems is that they operate in isolation and so do not fully benefit a country's health status. This paper highlighted that South Africa is currently in need of a patient-centric health system that will promote preventative care and aid in improving the quality of care. The use of a mobile PHR was suggested because of the fact that South Africans have high access to the Internet via their mobile phones. Achieving this, however, will require a lot of collaboration from all parties involved in the care of an individual.

Healthcare systems exist but for as long as they work in isolation they will not yield the results that the South African health system is currently in need of. Interoperability between these systems would play an important role in ensuring that they communicate together in order to provide a better health system. Universal standards need to be adopted by the different organizations that participate in providing healthcare systems so as to reach the goal of integration and interoperability. This in turn will offer a faster and more efficient method of improving the patient care process. CC has proven to be another vehicle that can drive better collaboration between systems. Healthcare stands to benefit from this technology not only through better communication between health systems but it can also cut operational costs.

4. Conclusion

The lack of design guidelines for a PHR system aimed at the South African context has led to the problem of not having a PHR specifically designed for the country. This plays a role in the poor adoption rates of PHRs in South Africa. The suggested design considerations in this paper may guide PHR developers and relevant stakeholder when designing a PHR for the South African market. Such a PHR has the potential of improving the current state of health for South Africa through better decision-making, diagnosis and treatment, which will yield better health outcomes.

The high usage of mobile phones by South Africans to access the Internet and the great need for a highly curative approach expressed by the National Department of South Africa advocates for the need of a mobile PHR in South Africa. The use of CC and the implementation of eHealth standards provide means to make this system both interoperable and affordable.

This explorative study highlights design considerations for PHRs based on a thorough literature review. Future research will focus on gathering primary data to further develop these design guidelines. There will also be a focus on establishing the functional requirements of a PHR that will better serve the needs of the South African market. Usability aspects related to the use of mPHRs on mobile devices will also be investigated.

5. References

Ahuja, SP, Mani, S & Zambrano, J 2012, 'A survey of the state of cloud computing in healthcare', *Network and Communication Technologies*, vol 1, no. 2, pp. 12-19.

Alagoz, F, Valdez, AC, Wilkowska, W, Ziefle, M, Dorner, S & Holzinger, A 2010, 'From cloud computing to mobile Internet, from user focus to culture and hedonism: The crucible of mobile health care and Wellness applications', *Pervasive Computing and Applications 5th International Conference*, IEEE, Maribor.

Archer, N, Fevrier-Thomas, U, Lokker , C, McKibbon, KA & Straus, SE 2011, 'Personal health records: a scoping review', *J Am Med Inform Assoc*, vol 8, no. 4, pp. 515-522.

Bahga, A & Madisetti, VK 2013, 'A Cloud-based Approach for Interoperable Electronic Health Records(EHRs)', *IEEE Journal of biomedical and health informatics*, vol 17, no. 5, pp. 894-906.

Caligtan, CA & Dykes, PC 2011, 'Electronic Health Records and Personal Health Records', *Seminars in Oncology Nursing*, vol 27, no. 3, pp. 218-228.

Department of Health & CSIR 2014, 'National Health Normative Standards Framework for Interoperability in eHealth in South Africa', Standard, 240075.

Department of Health 2004, 'National Health Act', Act, Department of Health, 61, Government Gazette, Cape Town.

Department of Health 2007, 'A policy on quality in health care for South Africa', Policy, Department of Health, Pretoria.

Department of Health 2011, 'National Health Insurance in South Africa', Policy paper, Department of Health.

Dinh, HT, Lee, C, Niyato, D & Wang, P 2013, 'A survey of mobile cloud computing:architecure,applications, and approaches', *Wireless communications and mobile computing*, vol 13, pp. 1587-1611.

Dohan, MS, Abouzahra, M & Tan, J 2014, 'Mobile Personal Health Records: Research Agenda for Applications in Global Health', *47th Hawaii International Conference on Systems Science*, IEEE, Waikoloa.

Garrett, P & Seidman, J 2011, *EMR vs EHR- What is the difference?*, viewed 29 July 2014, <http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/>.

Gong, C, Liu, J, Zhang, Q, Chen, H & Gong, Z 2010, 'The Characteristics of Cloud Computing', *2010 39th International Conference on Parallel Processing Workshops*.

Hargreaves, JS 2010, 'Will Electronic Personal Health Records Benefit Providers and Patients in Rural America?', *Telemedicine and e-Health*, vol 16, no. 2, pp. 167-176.

IDABC 2004, 'European Interoperability Framework for Pan-European E-Government Services', Luxembourg.

International Organization for Standardization 2004, *Home:iso.org*, viewed 12 August 2014, <http://www.iso.org/iso/home.htm>.

JoJo, S & Mostert-Phipps, N 2013, 'Awareness and interest in web-based personal health records', *Proceedings of the 15th annual conference on world wide web applications*, Cape Peninsula University of Technology, Cape Town.

Kharrazi, H, Chisholm, R, VanNasdale, D & Thompson, B 2012, 'Mobile Personal Health Records: An Evaluation of Features and Functionality', *International Journal of Medical Informatics*, vol 81, no. 9, pp. 579-593.

Kim, MI & Johnson, KB 2002, 'Personal health records: Evaluation of Functionality and Utility', *Journal of the American Medical Informatics Association*, vol 9, no. 2, pp. 171-180.

Kuo, A 2011, 'Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model', *Journal of Medical Internet Research*, vol 13, no. 3, pp. 622-645.

Li, M, Yu, S, Zheng, Y, Ren, K & Lou, W 2013, 'Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based EncryptionAttribute-Based Encryption', *IEEE transaction on parallel and distributed systems*, vol 24, no. 1, pp. 131-143.

Maglogiannis, I 2011, 'Towards the Adoption of Open Source and Open Access Electronic Health Record Systems', *Journal of Healthcare engineering*, vol 3, no. 1, pp. 141-161.

Maloney, F & Wright, A 2010, 'USB-based personal health records: an analysis of features and functionality', *International Journal of Medical Informatics*, vol 79, no. 2, pp. 97-111.

Mell, P & Grance, T 2011, 'The NIST Definition of Cloud Computing', U.S. Department of Commerce, National Institute of Standards and Techology, National Institute of Standards and Technology, Gaithersburg, MD.

Moore, J 2009, *HIEs, Future PaaS for Healthcare?*, viewed 07 August 2014, <http://www.chilmarkresearch.com/2009/11/02/hies-future-paas-for-healthcare/>.

Mostert-Phipps, N 2012, 'Health information technologies for improved continuity of care : a South African perspective', PhD Thesis, Faculty of Engineering,the Built Environment and Information Technology, Nelson Mandela Metropolitan University, Port Elizabeth.

Pagliari, C, Detmer, D & Singleton, P 2007, 'Potential of electronic personal health records', *BMJ*, vol 335, no. 330, pp. 330-333.

Pottas, D & Mostert-Phipps, N 2012, 'Citizens and personal health records: the case of Nelson Mandela Bay', *Studies in health technology and informatics*, vol 192, pp. 501-504.

Preuveneers, D & Berbers, Y 2008, 'Mobile Phones Assisting With Health Self-Care: a Diabetes Case Study', *10th international conference on Human computer interaction with mobile devices and services*.

Schweitzer, EJ 2014, 'Reconciliation of the cloud computing model with US federal electronic health record regulations', *Journal of the American Medical Informatics Association*, vol 19, no. 2, pp. 161-165.

South Africa 2012-2016, 'eHealth Strategy South Africa', National Department of Health.

Statistics South Africa 2013, 'General Household Survey', Statistical release, P0318.

Sultan, N 2014, 'Making use of cloud computing for healthcare provision: opportunities and challenges', *International journal of information management*, vol 34, no. 2, pp. 177-184.

Tang, PC, Ash, JS, Bates, W, Overhange, JM & Sands, DZ 2006, 'Personal health records:definitions,benefits, and strategies for overcoming barriers', *J AM Med Inform Assoc*, vol 13, no. 2, pp. 121-126.

Tang, PC & Lansky, D 2005, 'The Missing Link: Bridging The Patient–provider health information gap', *Health affairs*, vol 24, no. 5, pp. 1290-1295.

The Markle Foundation 2003, 'Connecting for health: A Public-Private Collaborative', Final report.

The Markle Foundation 2004, 'Connecting Americans to their health', Final report.

van der Westhuizen, E & Pottas, D 2010, 'Towards characteristics of lifelong health records', in H Takeda (ed.), *E-Health*, Springer, Berlin.

van Heerden, A, Tomlinson, M & Swartz, L 2012, 'Point of care in your pocket: a research agenda for the field of m-health', *Bulletin of the World Health Organization*, vol 90, no. 5, pp. 393-394.

World Health Organization, *eHealth*, viewed 29 July 2014, <http://www.who.int/ehealth/en/>.

Wynia, M & Dunn, K 2010, 'Dreams and nightmares: Practical and ethical issues for patients and physicians using personal health records', *The journal of law,medicine and ethics*, vol 38, no. 1, pp. 64-73.

Zhang, R & Liu, L 2010, 'Security Models and Requirements for Healthcare Application Clouds', *2010 IEEE 3rd International Conference on Cloud Computing*.

APPENDIX C1 – Part 1 background document for the elite interviews

Information security risk factors impacting PHR dimensions

1. Introduction

A Personal Health Record (PHR) is a tool, usually web-based, that allows individuals to capture, share, store and process their medical records in one central place (Kaelber, Jha, Johnston, Middleton, & Bates, 2008; Pagliari, Detmer, & Singleton, 2007; Sunyaev, Kaletsch, Mauro, & Krcmar, 2009). The PHR is typically owned, created and managed by the individual and allows him to have a lifelong summary of all of his health information in one convenient place. Such a system allows individuals to better manage their health and is especially useful for individuals with chronic conditions such as diabetes and hypertension, or with diseases such as cancer, tuberculosis or HIV/AIDS (Archer, Fevrier-Thomas, Lokker, McKibbon, & Straus, 2011).

In order for a PHR to be deemed useful, it has to satisfy the requirements associated with nine (9) dimensions, as identified by van der Westhuizen (2012). The table below gives a brief description on each of these dimensions.

DIMENSION	REQUIREMENT
CONFIDENTIALITY	PHRs must only be accessible to authorised parties.
INTEGRITY	No unauthorised additions, deletions or alterations. Edits must be tracked by auditing logs.
AVAILABILITY	PHRs must be accessible to both the individual and physician (if access is granted) all the time. Emergency access must also be enabled.
AUDITABILITY	PHRs should contain audit logs to track access, changes, additions and deletions. They must also support non repudiation.
ACCURACY	Information must be captured accurately and correctly by implementing tools that prevent human error.
COMPLETENESS	PHRs must not only contain basic personal information, physician visits, check-up notes and diagnoses, but also information such as diet and exercise logs, health insurance information, etc. in order for them to be considered complete.
APOMEDIATION	PHRs should educate individuals and assist them in capturing the

	record with a sense of understanding. Individuals must also have the ability to interact with one another and with physicians.
PRIVACY	An individual must have the ability to grant or revoke (including legally) access to his PHR.
INTEROPERABILITY	Ability to interoperate with other health systems so as to interchange health information. Importing and exporting of data into health standards must also be enabled in a PHR.

Table 1: PHR Dimensions(van der Westhuizen, 2010)

As PHRs are web-based, there are numerous ways in which the data can be stored on the internet and cloud computing is one of them (Osterhaus, 2010). Cloud computing can succinctly be defined as a broad array of pay-as-you-go applications delivered as a service over the internet, as well as the hardware and software used in the data centres that provide such services (Geelan, 2009; Sabahi, 2011).

Storing PHRs in the cloud exposes the users' data to numerous security and privacy risks (AbuKhousa, Mohamed, & Al-Jaroodi, 2012; Subashini & Kavitha, 2011). PHR providers need to know what to consider when they select a Cloud Service Provider (CSP) to ensure that sensitive PHR data will be kept private and secure. Even though countries have data protection laws that can protect the users' rights, they are not very effective to cloud computing services because data in the cloud can be stored anywhere in the world so jurisdictions have different laws (Svantesson & Clarke, 2010).

There are various information security risk factors that have an impact on the PHR dimensions highlighted in Table 1. These information security risk factors and the PHR dimensions that they have an impact on will be described in the next section.

2. Information security risk factors that have an impact on PHR dimensions

According to the context in which van der Westhuizen (2010) presented the PHR dimensions, some of them were found to be irrelevant in terms of potential information security risk factors. Completeness, apomediation and accuracy were thus not considered when identifying potential information security risk factors. The reasoning behind these exclusions are provided below:

- **Completeness** in this context pertains to the information that users are able to capture in a PHR, e.g. basic personal information, diagnosis details, allergies, and so forth. This dimension relates to the functionality offered by the PHR, in other words, whether it allows a user to capture enough detail to accurately represent his health history. Since this dimension does not relate to the availability of the information captured in the PHR but rather involves the option to capture the information, there are no information security risk factors associated with this dimension.

- **Apomediation** is the ability of a PHR to educate individuals about health matters and to assist them in interacting with their physicians – hence there are no information security risk factors that can have an impact on this dimension. Similar to the 'completeness' dimension, this dimension rather relates to the functionality offered by a PHR.
- **Accuracy** is required because a PHR should be able to prevent human error when an individual captures health information on the system and implements various tools to ensure accurate data capturing. Since this dimension again refers to the functionality included in the PHR, there are no information security risk factors associated with this dimension.

The PHR dimensions that may thus potentially be affected by information security risk factors are:

- Confidentiality
- Integrity
- Availability
- Auditability
- Privacy
- Interoperability

Table 2 illustrates information security risk factors that may have an impact on the relevant PHR dimensions, followed by a discussion on each risk factor.

RISK FACTORS	PHR DIMENSIONS					
	Confidentiality	Integrity	Availability	Auditability	Privacy	Interoperability
Malicious insiders	✓	✓	✓	✓	✓	
Third-party access	✓	✓	✓	✓	✓	
Multi-tenancy	✓	✓	✓		✓	
Software intrusion	✓		✓		✓	
Physical intrusion	✓	✓	✓		✓	
Poor encryption key management	✓		✓		✓	
Temporary outages			✓			
Prolonged and permanent outages			✓			
Data lock-in						✓
Denial of Service (DoS)			✓			

Table 2: Information Security risk factors vs. PHR dimensions

2.1. Malicious insiders

The staff members of a CSP may abuse their access to a PHR to perform malicious attacks. The threat of malicious insiders is amplified in cloud computing because of how information technology services and customers are all in one management domain (Mahajan & Sharma, 2015). The fact that the insider has more than enough time to study and understand the CSP's system makes it difficult to predict and detect the threat in time (Modi et al., 2013).

Below follows a list of the dimensions that are affected by this risk and where possible, examples are given for each dimension to emphasise how malicious insiders pose a risk to PHR data.

- **Confidentiality** – The confidentiality of a PHR can be compromised if the data is somehow leaked or if there is a misapplication of network rights. A malicious insider may gain access to sensitive information stored in the cloud in order to sell it or sabotage the company (Claycomb & Nicoll, 2012). This type of breach is hard to detect because the person already has direct access to the system (Modi et al., 2013).
- **Integrity** – The integrity of a cloud-based PHR may be compromised when a malicious insider with authorised access makes unauthorised modifications to the PHR or even to the software applications in the cloud. A disgruntled employee may

intentionally modify a program when certain conditions are met or during a certain period of time (Zissis & Lekkas, 2012).

- **Availability** – An incident is reported on where a system administrator in a cloud environment managed data and operations for other companies. The administrator removed critical software which prevented the provider from responding to customer request. This affected access to the customer data and thus availability (Claycomb & Nicoll, 2012). Cloud-based PHRs can also be affected by this risk when their CSP has malicious insiders.
- **Auditability** – It is vital that PHR systems should adhere to auditability for as long as the information is stored in them (Fernández-Alemán, Señor, Lozoya, & Toval, 2013). A system audit can be defined as a one-time or periodic occurrence to assess security (Krutz & Vines, 2010). A disgruntled employee may launch a distributed denial-of-service attack on his organisation in order to obstruct an audit and limit a forensic analysis of his malicious activities (Claycomb & Nicoll, 2012).
- **Privacy** – Data security and privacy are recognised as major concerns for PHRs (Kharrazi, Chisholm, VanNasdale, & Thompson, 2012). When individuals are not sure why their personal information is requested, who has access to it and how it will be used, they develop trust issues (Pearson & Benameur, 2010). This lack of trust can be a key inhibitor to the adoption of cloud services, especially when it comes to processing confidential or sensitive information such as health information. There is much legal uncertainty about privacy rights in the cloud, as privacy laws vary according to the jurisdiction in which the information resides at a particular time when stored in the cloud (Pearson & Benameur, 2010). The privacy challenge for software engineers of cloud services is to design the services in a manner that decreases privacy risks and ensures legal compliance (Ramgovind, Eloff, & Smith, 2010). It is possible for a malicious insider to knowingly access and release patients' sensitive health information to outsiders out of spite or revenge, which is a serious violation of privacy.

2.2. Third-party access

The CSP may outsource some functions, like storage, to a third party. This automatically creates a greater pool of people who have access to the users' PHR system. Below are the dimensions affected by this risk and examples will also be given for each in order to emphasise how third-party access poses a risk to PHR data:

- **Confidentiality:** A third party acting as a rogue administrator may access the servers of the CSPs and gain access to the customers' PHRs. An example of such an attack is that of a system administrator of a data-mining firm that used to have access to the servers and data that belonged to the victim organisation. The attacker downloaded millions of personal records that belonged to the customers of the victim organisation (Claycomb & Nicoll, 2012). This type of attack compromises the confidentiality of information and could easily happen to a CSP that is storing PHRs.

- **Integrity:** One needs to be sure that information has not been altered in any way throughout the capture, storage and communication process (Waegemann, 1996). Integrity may be compromised by a third party that decides to modify the contents of the PHR without being granted permission to do so by the owner. A certain cell phone provider that stored customer data in a Microsoft subsidiary cloud was unavailable when the provider lost the data. Thus the level of data integrity was not guaranteed, should that data be restored (Paquette, Jaeger, & Wilson, 2010).
- **Availability:** It is possible that the third party that stores PHR data may be unavailable due to many reasons. In 2008, it was reported that a CSP ceased operation without giving adequate notice to its customers. It was further reported that 45% of the data's safety was not guaranteed in terms of it being available or being restored (Paquette et al., 2010). If such a provider is a third-party that stores PHR data, this can lead to problems with regard to the care of a patient as his health record will cease to exist. The third party may also decide to hold the data hostage if there is a dispute with the CSP (Ashktorab & Taghizadeh, 2012).
- **Auditability:** An audit can be performed by internal or external auditors and it can be the responsibility of the CSP, the customer or even both. When the CSP outsources some services to a third party, auditing may be difficult because some functions may not be transparent enough for inspection (Choubey, Dubey, & Bhattacharjee, 2011).
- **Privacy:** The third party that stores the CSP's data may store it anywhere in the world. This raises privacy concerns for cloud-based PHRs because the PHR owners will not necessarily know where their data is stored. Different privacy laws apply for different jurisdictions, so it may be difficult to access data or move it from one country to another (Subashini & Kavitha, 2011).

2.3. Multi-tenancy

The nature of cloud computing allows different customers to share resources such as storage and processing and this creates an opportunity for malicious users to gain access to other users' data (Subashini & Kavitha, 2011). Below are the dimensions affected by this risk, as well as examples for each in order to emphasise how multi-tenancy poses a risk to PHR data:

- **Confidentiality:** Protected data may be exposed to an adversary, hence compromising confidentiality. A pertinent example is that of a cloud user that reads another user's workflow without permission (Saripalli & Walters, 2010). This may also happen to someone's PHR data.

- **Integrity:** An adversary can gain access to a PHR via the multi-tenant environment and perform unauthorised changes to the data, thus affecting its integrity (Carroll, Van Der Merwe, & Kotzé, 2011).
- **Availability:** Service and data availability is vital for healthcare providers who use cloud applications to access their patient data (AbuKhousa et al., 2012).
- **Privacy:** Data stored in the cloud is accessible to other users due to the sharing of resources. The PHR data may be accessed by an unauthorised user and this raises a privacy threat that may lead to medical identity theft, private medical data being made available to unauthorised parties, and so forth (Adhikari, Richards, & Scott, 2014).

2.4. Software intrusions

The cloud environment is prone to malicious software attacks due to the fact that it is hosted on the web (Singh, 2014). The PHR dimensions affected by this risk are listed below, together with examples for each in order to emphasise how software intrusions pose a risk to PHR data:

- **Confidentiality:** Unauthorised access to the cloud environment may affect the confidentiality of the data contained therein. An example is given of an outside attacker that gained access to an organisation's system by obtaining the credentials of one of the employees. The attacker gained access by tricking the employee into opening a document infected with malware, which gave him access to the organisation's email service (Claycomb & Nicoll, 2012).
- **Availability:** The cloud is vulnerable to zombie attacks. An attacker tries to bombard the victim by sending requests from innocent hosts (zombies) in the network. This type of attack may interrupt the expected behaviour of the cloud, which affects availability (Modi et al., 2013). Availability is crucial for PHR applications.
- **Privacy:** Phishing is used to trick users into exposing their data by manipulating them to click on a false link that redirects from the page they were currently accessing (Harkins, 2013; Modi et al., 2013). It is possible in the cloud environment to hijack accounts and services of cloud users and thus to expose sensitive data that should not be revealed (Modi et al., 2013).

2.5. Physical intrusions

Cloud computing services can be disrupted by threats caused by unauthorised physical access to the data centres where data is stored (Paquette et al., 2010). The PHR dimensions affected by this risk are listed below:

- **Confidentiality:** Data theft in the cloud data centre may lead to a breach in confidentiality as the information contained there may be accessed by unauthorised individuals (Kumar, Akash, Somesh, & Dewangan, 2013).

- **Integrity:** It is vital to ensure that the physical data centres that store cloud data are protected from theft, modification and fabrication (Zissis & Lekkas, 2012). This extends to the network architecture through which the data travels. Network attacks pose a threat not only to traffic coming towards the cloud, but also between cloud hosts (Singh & Pandey, 2013).
- **Availability:** This refers to data, software and also hardware resources being available to authorised users when needed (Zissis & Lekkas, 2012). Hardware theft of cloud resources has a huge impact on the efficiency and productivity of cloud services (Singh & Pandey, 2013), as it may lead to a loss of both data and hardware.
- **Privacy:** The storage of cloud data at remote third-party data centres gives rise to security issues such as privacy breaches (Subashini & Kavitha, 2011). The CSP that stores the PHR data may well have full control over it, thus allowing privacy violation (Kumar et al., 2013).

2.6. Poor encryption key management

Users of cloud services have the option to encrypt their own data (AbuKhousa et al., 2012), and therefore there is the possibility of the disclosure or loss of the encryption keys. The PHR dimensions affected by the risk of poor encryption key management are listed below:

- **Confidentiality:** Using a single key to encrypt data and sharing the key with the different parties that have access to the data may cause confidentiality problems. A malicious or compromised cloud user may gain access to the key by pretending to be a legitimate user (Puttaswamy & Zhao, 2011).
- **Availability:** Data in the cloud resides in a shared environment due to multi-tenancy and service providers that all have access to it. Inadequate encryption or poor management of the encryption keys may lead to data loss and unavailability of the data when needed (Carroll et al., 2011).
- **Privacy:** Ideally it is the data owners who are responsible for key management, but if the users of cloud services do not have adequate expertise to manage their encryption keys, they may entrust their CSPs to perform this task (Chen & Zhao, 2012). This may raise privacy concerns because it means the CSP has unlimited access to private information and may compromise it.

2.7. Temporary outages

Even though cloud computing is known for its high level of service reliability and availability, it can and does experience outages (Leavitt, 2009). The PHR dimension affected by this risk is given below, together with examples of each in order to emphasise how temporary outages pose a risk to PHR data:

- **Availability:** In 2008, a temporary outage was witnessed in the three-hour outage that affected Amazon's Simple Storage Service. This consequently affected Twitter and other companies using the service. Cloud services may also be affected by connectivity and bandwidth speed limitations. PHR data needs to be accessible at all times, especially during emergency situations. An outage may affect the care of a patient (Jansen, 2011).

2.8. Prolonged and permanent outages

A CSP may experience problems such as bankruptcy or facility loss, which may lead to the unavailability of services for extended periods, if not forever (Jansen, 2011). The PHR dimension affected by this risk is given below, together with an example in order to emphasise how prolonged and permanent outages pose a risk to PHR data:

- **Availability:** Also in 2008, an online storage provider named Omnidrive closed without warning its users. This affected the availability of their data with that provider (Jansen, 2011). Patients need to always have a record of their health data. Losing a PHR means losing a lifetime of information as it is collected over a long period of time.

2.9. Data lock-in

Data lock-in is caused by the loss of portability of the customer's data and programs (Tripathi & Mishra, 2011). The PHR dimension affected by this risk is given below; together with an example in order to emphasise how data lock-in poses a risk to PHR data:

- **Interoperability:** If the current CSP runs out of business while storing customer data, customers are not able to retrieve their data and move it to another provider (Tripathi & Mishra, 2011). When Google Health was discontinued in January 2012, its users had a year to download their health data. However, most infrastructures in the cloud do not support interoperability between their data, applications and services. This makes it difficult to move the PHR data to another provider or in-house IT environment (Kuo, 2011).

2.10. Denial of Service (DoS)

This occurs when an attacker sends bogus requests to the server to cause an overflow that will block legitimate requests from reaching the server – thus making its services unavailable (Jansen, 2011). The PHR dimension affected by this risk is given below; together with an example in order to emphasise how data lock-in poses a risk to PHR data:

- **Availability:** An example in this regard is that of a code-hosting site called BitBucket which had an outage for over 19 hours due to a DoS attack on the Amazon infrastructure that it uses (Modi et al., 2013). Depending on the extent to which a patient is reliant on PHR data, loss of availability may have a huge impact.

The above section provided the PHR information security risk factors that may impact PHR dimensions.

3. Conclusion

This document provided a brief background on the research study at hand. It highlighted the identified PHR dimensions and how they can be impacted by information security risk factors.

References

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Challenges. *Future Internet*, *4*(3), 621–645. http://doi.org/10.3390/fi4030621

Adhikari, R., Richards, D., & Scott, K. (2014). Security and Privacy Issues Related to the Use of Mobile Health Apps. *25th Australasian Conference on Information Systems (ACIS 2014)*, (Schulke 2013).

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. a, & Straus, S. E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 515–522. http://doi.org/10.1136/amiajnl-2011-000105

Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *1*(2), 234–245.

Carroll, M., Van Der Merwe, A., & Kotzé, P. (2011). Secure Cloud Computing: Benefits, Risks and Controls. *Information Security for South Africa*, 1–9. http://doi.org/10.1109/ISSA.2011.6027519

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*, *1*(973), 647–651. http://doi.org/10.1109/ICCSEE.2012.193

Choubey, R., Dubey, R., & Bhattacharjee, J. (2011). A survey on cloud computing security, challenges and threats. *International Journal on Computer …*, *3*(3), 1227–1231. Retrieved from http://www.doaj.org/doaj?func=fulltext&aId=719357

Claycomb, W. R., & Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. *Proceedings - International Computer Software and Applications Conference*, 387–394. http://doi.org/10.1109/COMPSAC.2012.113

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. http://doi.org/10.1016/j.jbi.2012.12.003

Geelan, J. (2009). Twenty-One experts define Cloud computing. Retrieved February 18, 2014, from http://www.vertualization.sys-con.com/node/612375?page=0,0

Harkins, M. (2013). *Managing Risk and Information Security*. http://doi.org/10.1007/978-1-4302-5114-9

Jansen, W. a. (2011). Cloud hooks: Security and privacy issues in cloud computing. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. http://doi.org/10.1109/HICSS.2011.103

Kaelber, D., Jha, A., Johnston, D., Middleton, B., & Bates, D. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, *15*(6), 729–736. http://doi.org/10.1197/jamia.M2547.Introduction

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: an evaluation of features and functionality. *International Journal of Medical Informatics*, *81*(9), 579–93. http://doi.org/10.1016/j.ijmedinf.2012.04.007

Krutz, R., & Vines, R. (2010). *Cloud security- A comprehensive guide to secure cloud computing*. Wiley Publishing Inc.

Kumar, K., Akash, D., Somesh, W., & Dewangan, K. (2013). A Valued Analysis of Information Security , Threats and Solutions for Cloud Computing, *2*(9), 648–658.

Kuo, A. M. (2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model. *Journal of Medical Internet Research*, *13*(3). http://doi.org/10.2196/jmir.1867

Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? *Growth Lakeland*, *42*(January), 15–20. http://doi.org/10.1109/MC.2009.20

Mahajan, a, & Sharma, S. (2015). The Malicious Insiders Threat in the Cloud. *Oaji.Net*, *3*(2),

245–256. Retrieved from http://oaji.net/articles/2015/786-1431229638.pdf
Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, *63*(2), 561–592. http://doi.org/10.1007/s11227-012-0831-5
Osterhaus, L. C. (2010). Cloud Computing and Health Information. *U of I SLIS Journal*, *19*, 1–7.
Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. *Bmj*, *335*(7615), 330–333. http://doi.org/10.1136/bmj.39279.482963.AD
Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. http://doi.org/10.1016/j.giq.2010.01.002
Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. http://doi.org/10.1109/CloudCom.2010.66
Puttaswamy, K. P. N., & Zhao, B. Y. (2011). Silverline : Toward Data Confidentiality in Storage-Intensive Cloud Applications. *Access*, 1–13. http://doi.org/10.1145/2038916.2038926
Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in Cloud computing. *Information Security for South Africa (ISSA), 2010*. http://doi.org/10.1109/ISSA.2010.5588290
Sabahi, F. (2011). Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 245–249. http://doi.org/10.1109/ICCSN.2011.6014715
Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. *2010 IEEE 3rd International Conference on Cloud Computing*, 280–288. http://doi.org/10.1109/CLOUD.2010.22
Singh, J. (2014). Cyber-Attacks in Cloud Computing : A Case Study, *1*(2), 78–87.
Singh, V., & Pandey, S. K. (2013). CLOUD SECURITY RELATED THREATS, *4*(9), 2571–2579.
Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006
Sunyaev, A., Kaletsch, A., Mauro, C., & Krcmar, H. (2009). Security Analysis of the German Electronic Health Card ' S Peripheral Parts. In *International Conference on Enterprise Information Systems* (pp. 19–26).
Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law and Security Review*, *26*(4), 391–397. http://doi.org/10.1016/j.clsr.2010.05.005
Tripathi, A., & Mishra, A. (2011). Cloud computing security considerations. *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1–5. http://doi.org/10.1109/ICSPCC.2011.6061557
van der Westhuizen, E. (2010). *A framework for Personal Health Records in Online Social Networking*. Nelson Mandela Metropolitan University.
Waegemann, C. P. (1996). IT security: developing a response to increasing risks. *International Journal of Bio-Medical Computing*, *43*(1-2), 5–8. http://doi.org/10.1016/S0020-7101(96)01220-2
Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. http://doi.org/10.1016/j.future.2010.12.006

APPENDIX C2 – Part 1 questionnaire the elite interviews

Nelson Mandela Metropolitan University

for tomorrow

PHR Dimensions Elite Interview Questionnaire

The purpose of this questionnaire is to obtain expert perspectives and feedback on the quality and overall impression of the classification of information security risk factors that may potentially impact PHR dimensions, as described in the Background document provided to you. If you have any queries concerning the questionnaire, you can contact me at: 209029505@live.nmmu.ac.za

Please refer to Table 2 and the discussion of the PHR dimensions as provided in the background document before completing this questionnaire.

1. Reviewer Demographics

Please provide the following details about yourself:

1.1. Title and full name: Click here to enter text.

1.2. What is your current job title? Click here to enter text.

1.3. What are your areas of expertise? Click here to enter text.

1.4. How many years' experience do you have in the field of Health Informatics (for example Personal Health Records)? Click here to enter text.

1.5. Please indicate your level of knowledge in the field of Health Informatics (for example Personal Health Records) Choose an item.

1.6. How many years' experience do you have in the field of Information Security? Click here to enter text.

1.7. Please indicate your level of knowledge in the field of Information Security Choose an item.

1.8. Please provide any further information related to your professional status and any knowledge levels that you feel are relevant to this review process. Click here to enter text.

2. Quality of the classification of information security risk factors impacting PHR dimensions

For each of the questions below please indicate your level of agreement on a scale of 1-5:
1 - Strongly disagree
2 - Disagree
3 - Somewhat agree
4 - Agree
5 - Strongly agree
Please motivate your level of agreement where possible.

2.1. Do you agree that the threat of "Malicious Insiders" can impact the Confidentiality, Integrity, Availability, Auditability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.2. Do you agree that the threat of Third-party access can impact the Confidentiality, Integrity, Availability, Auditability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.3. Do you agree that the threat of Multi-tenancy can impact the Confidentiality, Integrity, Availability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.4. Do you agree that the threat of Software intrusions can impact the Confidentiality, Availability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.5. Do you agree that the threat of Physical intrusions can impact the Confidentiality, Integrity, Availability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.6. Do you agree that the threat of Poor encryption key management can impact the Confidentiality, Availability and Privacy of a PHR?
Choose an item. Click here to enter text.

2.7. Do you agree that the threat of Temporary outages can impact the Availability of a PHR?
Choose an item. Click here to enter text.

2.8. Do you agree that the threat of Prolonged and permanent outages can impact the Availability of a PHR?
Choose an item. Click here to enter text.

2.9. Do you agree that the threat of Data lock-in can impact the Interoperability of a PHR?
Choose an item. Click here to enter text.

2.10. Do you agree that the threat of Denial of Service (DoS) can impact the Availability of a PHR?
Choose an item. Click here to enter text.

3. Efficacy of the classification of information security risk factors impacting PHR dimensions

3.1. In your opinion, do you think this classification of information security risk factors that may potentially impact PHR dimensions is adequate? Would you link the risk factors and dimensions differently?
Click here to enter text.

4. Overall Impression

4.1. Please provide any final comments, criticism or suggestions.
Click here to enter text.

Thank you for your input regarding the classification of information security risk factors that may potentially impact PHR dimensions. Your contribution will provide valuable insight into their value as an output for this research.

Please save and submit this document via e-mail at: s209029505@live.nmmu.ac.za

APPENDIX C3 – Part 1 completed questionnaire for the elite interviews

Nelson Mandela Metropolitan University

for tomorrow

PHR Dimensions Elite Interview Questionnaire

The purpose of this questionnaire is to obtain expert perspectives and feedback on the quality and overall impression of the classification of information security risk factors that may potentially impact PHR dimensions, as described in the Background document provided to you. If you have any queries concerning the questionnaire, you can contact me at: 209029505@live.nmmu.ac.za

Please refer to Table 2 and the discussion of the PHR dimensions as provided in the background document before completing this questionnaire.

1. Reviewer Demographics

Please provide the following details about yourself:

1.1. Title and full name: Click here to enter text.

1.2. What is your current job title? Deputy Director: ICT Service Delivery

1.3. What are your areas of expertise? Information Technology

1.4. How many years' experience do you have in the field of Health Informatics (for example Personal Health Records)? 3

1.5. Please indicate your level of knowledge in the field of Health Informatics (for example Personal Health Records) (3) Knowledgeable

1.6. How many years' experience do you have in the field of Information Security? 17

1.7. Please indicate your level of knowledge in the field of Information Security (4) Very knowledgeable

1.8. Please provide any further information related to your professional status and any knowledge levels that you feel are relevant to this review process. Completed my Masters degree in the field of PHR's

2. Quality of the classification of information security risk factors impacting PHR dimensions

For each of the questions below please indicate your level of agreement on a scale of 1-5:
1 - Strongly disagree
2 - Disagree
3 - Somewhat agree
4 - Agree
5 - Strongly agree
Please motivate your level of agreement where possible.

2.1. Do you agree that the threat of "Malicious Insiders" can impact the Confidentiality, Integrity, Availability, Auditability and Privacy of a PHR?
3 - Somewhat agree Companies hosting the PHR solution need to provide non disclosure agreements between the individual and themselves. Otherwise this highly confidential personal information can be used in marketing campaigns and even potentially leaked into the hands of potential wrong doers.

2.2. Do you agree that the threat of Third-party access can impact the Confidentiality, Integrity, Availability, Auditability and Privacy of a PHR?
3 - Somewhat agree Third Party access needs to managed correctly. The PHR should be setup in such a way that the individual clearly understands what information will be made available to Third-parties. If the PHR scope is defined correcty, the threat will be mitigated and actually allow external medical practitioners with valuable information.

2.3. Do you agree that the threat of Multi-tenancy can impact the Confidentiality, Integrity, Availability and Privacy of a PHR?
4 - Agree Strict level of access control need to be defined with different category/roles of users

2.4. Do you agree that the threat of Software intrusions can impact the Confidentiality, Availability and Privacy of a PHR?
5 - Strongly agree With any software comes potential bugs and backdoors. This is the main threat to online PHR's.

2.5. Do you agree that the threat of Physical intrusions can impact the Confidentiality, Integrity, Availability and Privacy of a PHR?
3 - Somewhat agree Click here to enter text.

2.6. Do you agree that the threat of Poor encryption key management can impact the Confidentiality, Availability and Privacy of a PHR?
5 - Strongly agree This goes along with Software intrusion. Very similar as poor encryption management leads to hackers being able to access personal information and denial of service.

2.7. Do you agree that the threat of Temporary outages can impact the Availability of a PHR?

4 - Agree If the PHR isn't available consistently, the adoption of this electronic format will fail.

2.8. Do you agree that the threat of Prolonged and permanent outages can impact the Availability of a PHR?

4 - Agree Similar to previous question.

2.9. Do you agree that the threat of Data lock-in can impact the Interoperability of a PHR?

4 - Agree The vendor should at least adhere to ISO standards to allow export of PHR into approved standard format. Without proper interoperability, the whole meaning and purpose of the PHR will be lost.

2.10. Do you agree that the threat of Denial of Service (DoS) can impact the Availability of a PHR?

4 - Agree Any service is succeptable to DOS attacks and this will impact the availability.

3. Efficacy of the classification of information security risk factors impacting PHR dimensions

3.1. In your opinion, do you think this classification of information security risk factors that may potentially impact PHR dimensions is adequate? Would you link the risk factors and dimensions differently?

I am very impressed with the classifactions of the PHR dimensions and the omission of the 3 dimensions not effected by information security risk factors. The alignment of risk factors to PHR dimensions are easily understandable and I am in agreement.

4. Overall Impression

4.1. Please provide any final comments, criticism or suggestions.

A good piece of work. Perhaps look into the POPI act and how the requirements of this act will impact on information security pertaining to PHR's.

Thank you for your input regarding the classification of information security risk factors that may potentially impact PHR dimensions. Your contribution will provide valuable insight into their value as an output for this research.

Please save and submit this document via e-mail at: s209029505@live.nmmu.ac.za

APPENDIX D1 – Part 2 background document for the elite interviews

Guidelines for secure cloud-based Personal Health Records

1. Introduction

A Personal Health Record (PHR) is a tool, usually web-based, that allows individuals to capture, share, store and process their medical records in one central place (Kaelber, Jha, Johnston, Middleton, & Bates, 2008; Pagliari, Detmer, & Singleton, 2007; Sunyaev, Kaletsch, Mauro, & Krcmar, 2009). The PHR is typically owned, created and managed by the individual and allows him to have a lifelong summary of all of his health information in one convenient place. Such a system allows individuals to better manage their health and is especially useful for individuals with chronic conditions such as diabetes and hypertension, or with diseases such as cancer, tuberculosis or HIV/AIDS (Archer, Fevrier-Thomas, Lokker, McKibbon, & Straus, 2011).

As PHRs are web-based, there are numerous ways in which the data can be stored on the internet and cloud computing is one of them (Osterhaus, 2010). Cloud computing can succinctly be defined as a broad array of pay-as-you-go applications delivered as a service over the internet, as well as the hardware and software used in the data centres that provide such services (Geelan, 2009; Sabahi, 2011).

Based on the advantages offered by cloud computing PHR providers are increasingly leaning towards using the cloud as their storage facility (Ming, Shucheng, Kui, & Wenjing, 2010). The individual's health record can thus be stored in the cloud, which reduces operational costs for PHR providers. Table 1.1 clarifies the terms PHR provider, Cloud Service Provider (CSP), and PHR user as it will be used throughout this study.

Table 1: Definition of terms

Term	Description
PHR provider	The entity providing the PHR system for use by the PHR user (patient).
Cloud Service Provider (CSP)	The entity providing cloud services to the PHR provider.
PHR user	The person (patient) who makes use of a PHR to record his health history. The PHR user is the customer of the PHR provider.

Storing information in the cloud raises discomfort for the users and as such, people are rather sceptical of using this powerful tool (Armbrust et al., 2010). PHRs stored in the cloud are at a higher risk because of the security and privacy issues found in the cloud (AbuKhousa, Mohamed, & Al-Jaroodi, 2012). Data stored in a PHR can typically be divided into two categories, namely Personally Identifiable Information (PII) and Healthcare data. PII consists of information that can be used to identify, locate or contact an individual, e.g. name, address, telephone number, etc. Healthcare data is comprised of media files about the individual, such as scans, x-rays and other types of images and videos (Elmogazy & Bamasak, 2013). This type of information is highly sensitive and should be treated as such. The security and privacy issues in cloud computing may affect the Cloud Service Providers (CSPs), the developers and the users of cloud applications.

1.1. Problem description

Storing PHRs in the cloud exposes the users' data to numerous security and privacy risks (AbuKhousa et al., 2012; Subashini & Kavitha, 2011). When PHR providers transfer data to the cloud, they also transfer most of its control.

Little guidance is given to PHR providers to assist them in making an informed choice when they select a CSP for storage of their customers' PHR data. They need to know what to consider when they select a CSP to ensure that sensitive PHR data will be kept private and secure. Even though countries have data protection laws that can protect the users' rights, they are not very effective to cloud computing services because data in the cloud can be stored anywhere in the world so jurisdictions have different laws (Svantesson & Clarke, 2010).

1.2. Problem statement and main objective

There is a lack of guidance to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data is kept private and secure.

The main objective of the research in hand is to propose guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data remains private and secure.

In the section that follows, these guidelines are described.

2. Guidelines for secure cloud-based PHRs

Information security plays a role in ensuring that sensitive information – in this case personal health information – is treated with utmost care and protection. The ISO 27799:2008 standard for information security management in health (International Organization for Standardization, 2008), together with ISO 17090-3:2008 policy management of certification authority (International Organization for Standardization, 2009) was consulted to identify control measures that will enforce the security of cloud-based PHRs. The discussions that follow are structured according to the risk factors associated with cloud-based PHRs to indicate which guideline(s) will be applicable for each risk factor. Table 1 below presents a summary of the guidelines that can be employed to control each risk. The sources that were consulted in order to identify the relevant control measures for the risks are also presented in the table below. A discussion of the guidelines will be presented below the table.

Table 2: Formulation of the guidelines

Risk Factor	Guideline	Control Measures (ISO 27799:2008 & ISO 17090-3:2008)	Source
Malicious insiders	• Control access to PHR data	• Access control policy (7.8.1.2) • Roles and responsibilities; Screening; Terms and conditions of employment (7.5.1) • Management responsibilities; Information security awareness, education and training; Disciplinary process (7.5.2) • Terminating responsibilities and return of assets; Removal of access rights (7.5.3)	• Behl, 2011
Third-party access	• Assess risks involved with third parties	• Assessment of risks related to external parties (7.3.3.1) • Addressing security in third-party agreements (7.3.3.3) • Health information exchange policies and procedures and exchange agreements (7.7.8.1)	• Modi et al., 2013 • Sengupta, Kaulgud, & Sharma, 2011
Multi-tenancy	• Separate customer data	• Separation of development, test and operational facilities (7.7.1.4)	• Mishra et al., 2011 • Modi et al., 2013

Continuation of Table 2

Risk Factor	Guideline	ISO 27799:2008 & ISO 17090-3:2008 Control	Source
Software intrusion	• Prevent malicious code infections	• Controls against malicious code (7.7.4.1)	• Mahmood & Hill, 2011 • Wei et al., 2013
Physical intrusion	• Store PHR data in secure data centres	• Physical security perimeter (7.6.1.1)	• Hutchings et al., 2013
Poor encryption key management	• Adopt strong private key management techniques	• Private key backup (7.6.2.5) • Method of destroying private key (7.6.2.11) • Avoid loss, disclosure or unauthorised use of private keys. If any occurs, report immediately (7.9.6.4)	• AbuKhousa et al., 2012; • Alex Mu-hsing Kuo, 2011
Temporary outages	• Ensure business continuity • Consider loss of network impact	• Information security aspects of business continuity management (disaster recovery) (7.11) • Security of network services (7.7.6.2)	• AbuKhousa et al., 2012 • Fernández-Cardeñosa, De La Torre-Díez, López-Coronado, & Rodrigues, 2012 • Onwubiko, Rimal, Choi, & Lumb, 2010
Prolonged and permanent outages	• Backup and encrypt PHR data	• Health information backup (7.7.5)	• Jansen & Grance, 2011
Data lock-in	• Enforce technical interoperability	• Compliance with security policies, standards and technical compliance (7.12.3)	• Carroll et al., 2011 • Dillon, Wu, & Chang, 2010
Denial of Service (DoS)	• Report security incidents	• Reporting information security events and weaknesses (7.10.1)	• AbuKhousa et al., 2012 • Carroll et al., 2011 • Modi et al., 2013

In the discussions that follow the risk is first described, followed by the guideline that has been identified to limit the risk. In addition, the control measures as identified from the relevant ISO documents and highlighted in Table 2, are also discussed.

2.1. Malicious insiders

The insider threat is very common in the cloud environment and there is usually a lack of transparency about the hiring process of the CSP. There is no clarity about their hiring standards and practices, and this makes space for an opponent to gain access to sensitive information (Behl, 2011). The main guideline that has been identified to limit this risk is to **control access to PHR data**, which implies the following:

- In order to govern access to personal health information, an access control policy should be in place. It should be predefined according to the roles with associated authorities, which are consistent, but limited to the needs of that certain role (7.8.1.2).
- Prior to employment, staff members should be given roles and responsibilities in the job description. A screening process should also be conducted to verify identity, living address, previous employment, as well as terms and conditions of employment (7.5.1).
- During employment, staff members should be assigned responsibilities, offered information security awareness and training, and be informed of the disciplinary process (7.5.2).
- Upon termination or change of employment, access rights must be revoked (7.5.3).

2.2. Third-party access

Adding more administrators to cloud systems increases the risk of unauthorised access (Modi et al., 2013). The third party may pose a threat to the users of cloud services if he/she aims to use in a negative way the access that the CSP granted them. Other risks involved with third parties include maintaining data confidentiality and integrity (Sengupta et al., 2011). The guideline that has been identified to limit this risk is to **assess the risks involved with third parties**, which implies the following:

- Organisations that are responsible for processing health information must conduct a risk assessment to weigh the risks that may be brought by third parties to the systems and data. Security controls must subsequently be implemented according to the identified level of risk and to the technologies used (7.3.3.1).
- In an instance where a third party is granted access to process personal health information, there must be formal contracts that specify the confidential nature and value of the personal health information; security measures that must be

implemented and complied with; limitations to access these services by third parties; and the penalty that will apply should any of these be breached (7.3.3.3).
- Information exchange agreements that specify the minimum set of controls to be implemented must also be formulated (7.7.8.1).

2.3. Multi-tenancy

The lack of compartmentalisation of resources in cloud computing allows users to access other users' personal information (Mishra et al., 2011). Multi-tenancy also makes it difficult to monitor and log the processes of virtual machines in the cloud (Modi et al., 2013). The guideline that has been identified to deal with this risk is to **separate customer data**, which implies the following:

- Development, test and operation facilities should be separated physically or virtually (7.7.1.4).

2.4. Software intrusion

It is difficult to eliminate software vulnerabilities in the cloud and this raises concerns for prospective cloud customers. Malware also compromises the integrity of software in the cloud because it can modify the victim's software somehow (Mahmood & Hill, 2011). The guideline that has been identified to deal with this risk is to **prevent malicious code infections**, which implies the following:

- Proper prevention, detection and response controls that are used to protect systems against malicious software must be adopted and appropriate user awareness and training must be implemented (7.7.4.1).

2.5. Physical intrusion

The data centres that CSPs use to store the PHR data may be at risk of being attacked physically, which would result in hardware theft, unauthorised access to servers or loss of access to data (Hutchings et al., 2013). The guideline that has been identified to limit this risk is to **store PHR data in secure data centres**, which implies the following:

- A physical security perimeter should exist in order to control access to facilities that contain personal health information. There should be physical entry controls; offices should be secured; there should be protection against external and environmental threats; and public access, delivery and loading areas should be secure enough not to expose personal health information. These are all ways to prevent the public from getting too close to IT equipment. Software or equipment used to support a healthcare application that contains personal health information should not be removed from the site or relocated within the organisation without authorised permission from the organisation (7.6.1.1).

2.6. Poor encryption key management

Some systems allow users to generate their own decryption keys and distribute them to authorised parties (AbuKhousa et al., 2012). This becomes a challenge if the user loses the keys or discloses them to malicious parties (Kuo, 2011). For the purpose of the identified control measures, encryption keys are from this point onwards referred to as private keys and the party responsible for keeping the keys is known as the certificate holder. The guideline that has been identified to deal with this risk is to **adopt strong private key management techniques**, which implies the following:

- It is recommended that the certificate holder creates a backup of the private keys where possible. This backup will be held at the environment of the certificate holder and will be entirely in his control (7.6.2.5).
- When the private key is no longer in use, all its copies in computer memory and shared disk space must be securely destroyed by overwriting multiple times (7.6.2.11).
- A certificate holder must ensure that he/she makes every effort to avoid the loss, disclosure or unauthorised use of his private keys. If there is any actual or suspected loss, disclosure or other compromise of the private key, the certificate holder must immediately notify the certification authority (7.9.6.4).

2.7. Temporary outages

It is vital that systems that process health information in the cloud should be available continuously with no interruptions (AbuKhousa et al., 2012). Outages are not exclusive to cloud environments but they are highlighted there because of the interconnectedness of their services (Gonzalez et al., 2011). A temporary outage could be caused by a natural disaster, vulnerability exploits and deliberate attacks (Onwubiko et al., 2010). The guideline that has been identified to limit this risk is to **ensure business continuity**, which implies the following:

- Health organisations recognise business continuity management as a requirement, and this includes disaster recovery (7.11).
- They should carefully consider what impact the loss of network service availability will have on clinical practice (7.7.6.2).

2.8. Prolonged and permanent outages

When the cloud that is used for storage is unavailable for extended periods, it has a negative impact on the customer who relies on that data. It is important for a CSP to have a plan of how the data will be recovered and to ensure that it is still accessible (Jansen & Grance, 2011). The guideline that has been identified to limit this risk is to **back up and encrypt PHR data**, which implies the following:

- In order to make sure that personal health information will be available in future; it should be backed up and stored in a physically secure environment (7.7.5).

2.9. Data lock-in

It is possible for customer data to be locked in in the cloud due to a number of reasons – such as the provider going out of business (Carroll et al., 2011). The lack of interoperability between cloud services prohibits customers from utilising multiple providers at the same time (Dillon et al., 2010). The guideline that has been identified to deal with this risk is to **enforce technical interoperability**, which implies the following:

- Systems that process personal health information need to be technically interoperable as many of them typically consist of different interoperating systems (7.12.3).

2.10. Denial of Service (DoS)

Denial of Service (DoS) poses numerous threats in the cloud computing environment (Carroll et al., 2011). By attacking one server, the attacker may affect the availability of other services as well (Modi et al., 2013). This threat is intensified in a health system that becomes unavailable, especially in an emergency situation (AbuKhousa et al., 2012). The guideline that has been identified to limit this risk is to **report security incidents**, which implies the following:

- Organisations that process personal health information should report security incidents. These include corruption or unintentional disclosure of personal health information, or the loss of availability of health information systems, where such a loss affects patient care in an undesirable manner (7.10.1).

The above section provided the guidelines that can be used to control the risk factors and ultimately assist PHR providers in selecting a secure CSP for their customers' data.

3. Conclusion

This document provided a brief background on the research topic by highlighting the problem description, problem statement together with the formulation of the research output i.e. the guidelines. The information security risk factors were listed and the guidelines for each risk factor were provided and explained.

References

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health Cloud: Opportunities and Challenges. *Future Internet*, *4*(3), 621–645. http://doi.org/10.3390/fi4030621

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. a, & Straus, S. E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 515–522. http://doi.org/10.1136/amiajnl-2011-000105

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A view of Cloud Computing. *Communications of the ACM*, *53*(4), 50–58.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. *Proceedings of the 2011 World Congress on Information and Communication Technologies, WICT 2011*, 217–222. http://doi.org/10.1109/WICT.2011.6141247

Carroll, M., Van Der Merwe, A., & Kotzé, P. (2011). Secure Cloud Computing: Benefits, Risks and Controls. *Information Security for South Africa*, 1–9. http://doi.org/10.1109/ISSA.2011.6027519

Dillon, T., Wu, C. W. C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 27–33. http://doi.org/10.1109/AINA.2010.187

Elmogazy, H., & Bamasak, O. (2013). Towards healthcare data security in cloud computing. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 363–368. http://doi.org/10.1109/ICITST.2013.6750223

Fernández-Cardeñosa, G., De La Torre-Díez, I., López-Coronado, M., & Rodrigues, J. J. P. C. (2012). Analysis of cloud-based solutions on EHRs systems in different scenarios. *Journal of Medical Systems*, *36*(6), 3777–3782. http://doi.org/10.1007/s10916-012-9850-2

Geelan, J. (2009). Twenty-One experts define Cloud computing. Retrieved February 18, 2014, from http://www.vertualization.sys-con.com/node/612375?page=0,0

Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 231–238. http://doi.org/10.1109/CloudCom.2011.39

Hutchings, A., Smith, R. G., & James, L. (2013). Cloud computing for small business: Criminal and security threats and prevention measures, (456).

International Organization for Standardization. (2008). *Health informatics — Information security management in health using ISO/IEC 27002* (Vol. 2008). Switzeralnd.

International Organization for Standardization. (2009). *SANS 17090-3 : 2009 SOUTH AFRICAN NATIONAL STANDARD Health informatics — Public key infrastructure Part 3 : Policy management of certification authority*.

Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *Director*, *144*(7). http://doi.org/10.3233/GOV-2011-0271

Kaelber, D., Jha, A., Johnston, D., Middleton, B., & Bates, D. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, *15*(6), 729–736. http://doi.org/10.1197/jamia.M2547.Introduction

Kuo, A. M. (2011). Opportunities and challenges of cloud computing to improve health care services. *J Med Internet Res*, *13*(3), e67. http://doi.org/10.2196/jmir.1867

Kuo, A. M. (2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model. *Journal of Medical Internet Research*, *13*(3). http://doi.org/10.2196/jmir.1867

Mahmood, Z., & Hill, R. (2011). *Computer Communications and Networks*.

Ming, L., Shucheng, Y., Kui, R., & Wenjing, L. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *50 LNICST*, 89–106. http://doi.org/10.1007/978-3-642-16161-2_6

Mishra, A., Mathur, R., Jain, S., & Rathore, J. (2011). Cloud Computing Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *1*(1), 36–39.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, *63*(2), 561–592. http://doi.org/10.1007/s11227-012-0831-5

Onwubiko, C., Rimal, B. P., Choi, E., & Lumb, I. (2010). Cloud Computing. *Computer Communications*, *77*, 271–288. http://doi.org/10.1007/978-1-84996-241-4

Osterhaus, L. C. (2010). Cloud Computing and Health Information. *U of I SLIS Journal*, *19*, 1–7.

Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. *Bmj*, *335*(7615), 330–333. http://doi.org/10.1136/bmj.39279.482963.AD

Sabahi, F. (2011). Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 245–249. http://doi.org/10.1109/ICCSN.2011.6014715

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). Cloud Computing Security--Trends and Research Directions. *2011 IEEE World Congress on Services*, 524–531. http://doi.org/10.1109/SERVICES.2011.20

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006

Sunyaev, A., Kaletsch, A., Mauro, C., & Krcmar, H. (2009). Security Analysis of the German Electronic Health Card ' S Peripheral Parts. In *International Conference on Enterprise Information Systems* (pp. 19–26).

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law and Security Review*, *26*(4), 391–397. http://doi.org/10.1016/j.clsr.2010.05.005

Wang, L., Laszewski, G. Von, & Younge, A. (2010). Cloud computing: a perspective study. *New*

Generation …, *28*, 137–146. Retrieved from http://link.springer.com.e.bibl.liu.se/article/10.1007/s00354-008-0081-5

Wei, J., Pu, C., Rozas, C., Rajan, A., & Zhu, F. (2013). Modelling the runtime integrity of Cloud servers: A scoped invariant perspective. In *Privacy and security of Cloud Computing* (pp. 212–232). London: Springer.

APPENDIX D2 – Part 2 questionnaire for the elite interviews

Nelson Mandela Metropolitan University
for tomorrow

Elite Interview Questionnaire on Guidelines for secure cloud-based Personal Health Records

The purpose of this questionnaire is to obtain expert perspectives and feedback on the utility, quality, efficacy and overall impression of the guidelines for secure cloud-based Personal Health Records (PHRs) as described in the background document provided to you. If you have any queries concerning the questionnaire, you can contact me at: 209029505@live.nmmu.ac.za

Please refer to Table 2 and the discussion of the guidelines as provided in the background document before completing this questionnaire.

1. Reviewer Demographics

Please provide the following details about yourself:

1.1. Title and full name: Click here to enter text.

1.2. What is your current job title? Click here to enter text.

1.3. What are your areas of expertise? Click here to enter text.

1.4. How many years' experience do you have in the field of Cloud Computing Click here to enter text

1.5. Please indicate your level of knowledge in the field of Cloud Computing Choose an item.

1.6. How many years' experience do you have in the field of Health Informatics (for example Personal Health Records)? Click here to enter text.

1.7. Please indicate your level of knowledge in the field of Health Informatics (for example Personal Health Records) Choose an item.

1.8. How many years' experience do you have in the field of Information Security? Click here to enter text.

1.9. Please indicate your level of knowledge in the field of Information Security Choose an item.

1.10. Please provide any further information related to your professional status and any knowledge levels that you feel are relevant to this review process. Click here to enter text.

2. Utility of the guidelines for secure cloud-based Personal Health Records

2.1. Was the information provided in the document sufficient for a clear understanding of the need and function of the proposed guidelines?
Click here to enter text.

2.2. Was the description of the guidelines and control measures proposed to address the risks associated with cloud-based PHRs clear and easily understood? Click here to enter text.

2.3. Can these guidelines be easily understood and utilized by PHR providers to make an informed choice when selecting a cloud service provider to ensure that their customers' data is kept private and secure?
Click here to enter text.

2.4. Do you think these guidelines will be useful/ beneficial to PHR providers? Please elaborate on your answer. Click here to enter text.

3. Quality of the guidelines for secure cloud-based Personal Health Records

For each of the questions below please indicate your level of agreement on a scale of 1-5:
1 - Strongly disagree
2 - Disagree
3 - Somewhat agree
4 - Agree
5 - Strongly agree
Please motivate your level of agreement where possible.

3.1. (a) Do you agree that the threat of "Malicious Insiders" can be mitigated by the guideline "Control access to PHR data"?
Choose an item. Click here to enter text.
(b) Do you agree that the threat of "Malicious Insiders" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.1 in the background document?
Choose an item. Click here to enter text.

3.2. (a) Do you agree that the threat of "Third-party access" can be mitigated by the guideline "Assess risks involved with third parties"?
Choose an item. Click here to enter text.
(b) Do you agree that the threat of "Third-party access" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.2 in the background document?

Choose an item. Click here to enter text.

3.3. **(a) Do you agree that the threat of “Multi-tenancy” can be mitigated by the guideline “Separate customer data”?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of “Multi-tenancy” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.3 in the background document?
Choose an item. Click here to enter text.

3.4. **(a) Do you agree that the threat of “Software intrusions” can be mitigated by the guideline “Prevent malicious code infections”?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of “Software intrusions” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.4 in the background document?
Choose an item. Click here to enter text.

3.5. **(a) Do you agree that the threat of “Physical intrusions” can be mitigated by the guideline “Store PHR data in secure data centres”?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of “Physical intrusions” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.5 in the background document?
Choose an item. Click here to enter text.

3.6. **(a) Do you agree that the threat of “Poor encryption key management” can be mitigated by the guideline “Adopt strong private key management techniques”?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of “Poor encryption key management” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.6 in the background document?
Choose an item. Click here to enter text.

3.7. **(a) Do you agree that the threat of “Temporary outages” can be mitigated by the guidelines “Ensure business continuity” and “Consider loss of network impact”?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of “Temporary outages” can be mitigated by employing the control measures as indicated by the ISO

controls listed in Table 2 and as described in the bullet points under section 2.7 in the background document?
Choose an item. Click here to enter text.

3.8. **(a) Do you agree that the threat of "Prolonged and permanent outages" can be mitigated by the guideline "Backup and encrypt PHR data"?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of "Prolonged and permanent outages" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.8 in the background document?
Choose an item. Click here to enter text.

3.9. **(a) Do you agree that the threat of "Data lock-in" can be mitigated by the guideline "Enforce technical interoperability"?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of "Data lock-in" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.9 in the background document?
Choose an item. Click here to enter text.

3.10. **Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by the guideline "Report security incidents?**
Choose an item. Click here to enter text.
(b) Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.10 in the background document?
Choose an item. Click here to enter text.

4. Efficacy of the guidelines for secure cloud-based Personal Health Records

4.1. **In your opinion, are the guidelines adequate to assist PHR providers in making an informed choice when selecting a cloud service provider to ensure that their customers' data remains private and secure? Or are there other relevant aspects that need to be considered?** Click here to enter text.

4.2. **Do you think the use of these guidelines by PHR providers will contribute towards more secure cloud-based PHRs?** Click here to enter text.

4.3. **Do you agree that the different ISO standards used are adequate for the formation of the guidelines?** Click here to enter text.

5. Overall Impression

5.1. What is your overall opinion of the guidelines? Click here to enter text.

5.2. Can you recommend any way in which the guidelines can be improved? Click here to enter text.

5.3. Please provide any final comments, criticism or suggestions. Click here to enter text.

Thank you for your input regarding the guidelines for secure cloud-based Personal Health Records. Your contribution will provide valuable insight into their value as an output for this research, as well as allow the guidelines to be further improved.

Please save and submit this document via e-mail at: s209029505@live.nmmu.ac.za

APPENDIX D3 – Part 2 completed questionnaires for the elite interviews

Nelson Mandela Metropolitan University
for tomorrow

Elite Interview Questionnaire on Guidelines for secure cloud-based Personal Health Records

The purpose of this questionnaire is to obtain expert perspectives and feedback on the utility, quality, efficacy and overall impression of the guidelines for secure cloud-based Personal Health Records (PHRs) as described in the background document provided to you. If you have any queries concerning the questionnaire, you can contact me at: 209029505@live.nmmu.ac.za

Please refer to Table 2 and the discussion of the guidelines as provided in the background document before completing this questionnaire.

1. Reviewer Demographics

Please provide the following details about yourself:

1.1. Title and full name: Click here to enter text.

1.2. What is your current job title? Director of School (ICT)

1.3. What are your areas of expertise? Health Informatics and Information Security Management

1.4. How many years' experience do you have in the field of Cloud Computing 5

1.5. Please indicate your level of knowledge in the field of Cloud Computing (3) Knowledgeable

1.6. How many years' experience do you have in the field of Health Informatics (for example Personal Health Records)? 11 years

1.7. Please indicate your level of knowledge in the field of Health Informatics (for example Personal Health Records) Choose an item.

1.8. How many years' experience do you have in the field of Information Security? 20 years

1.9. Please indicate your level of knowledge in the field of Information Security (4) Very knowledgeable

1.10. Please provide any further information related to your professional status and any knowledge levels that you feel are relevant to this review process. None

2. Utility of the guidelines for secure cloud-based Personal Health Records

2.1. Was the information provided in the document sufficient for a clear understanding of the need and function of the proposed guidelines? Section 1, which provides this information, was entirely clear.

2.2. Was the description of the guidelines and control measures proposed to address the risks associated with cloud-based PHRs clear and easily understood? (1). The introductory part of Section 2 was very clear, except with regard to the "risk factors". I could not, from that section, deduce how the risk factors were identified. I later realised that the "Source" column in Table 2 indicated the source of the risk factors. Consider making clear in the introductory section that the risk factors were identified from literature which is specified in the "Source" column of Table 2. (2). The guidelines and control measures are clear as contained in Table 2. (3). There are some things in the detail description of the guidelines which are pointed out in questions 3.1 – 3.10 further below (where relevant).

2.3. Can these guidelines be easily understood and utilized by PHR providers to make an informed choice when selecting a cloud service provider to ensure that their customers' data is kept private and secure? The guidelines are structured according to the risk factors that were identified from literature. Thus the structure is centred around the WHY "of the guidelines". I think it would help the PHR providers if the guidelines are structured according to the WHAT "of the guidelines". Thus rather than providing the guidelines per risk factor, you could make change the headings to be the guideline headings (or guideline topic) and within that explain which risk factor or factors are addressed by the guideline. It would also be useful if the bullet points could be presented more structured. For example, identify topics within each guideline. Present the requirements for the guideline in a table. First column topic (sub-topic of guideline); second column description; last column relevant standard. You should keep the $, * and # that you used in Table 2, within the description of the guidelines. Lastly, although the guidelines are for the PHR providers, there are also things mentioned which the CSP must do ("the CSP should provide"). This is understandable as you want the PHR provider to know that they should check for this. Suggestion: Split the guidelines discussion within each topic between "what the PHR provider should do" and "what the CSP should do". These suggestions are simply to assist with a clear presentation of the guidelines which may help the PHR providers to more easily understand and use the guidelines.

2.4. Do you think these guidelines will be useful/ beneficial to PHR providers? Please elaborate on your answer. I definitely think that creating these guidelines will be both useful and beneficial to PHR providers because the information security controls that are required to address the risks are described in various standards, of which the PHR providers may not have the necessary expertise. The environment is complex in terms of both the risks and the possible controls thus these guidelines serve a useful purpose.

3. Quality of the guidelines for secure cloud-based Personal Health Records
For each of the questions below please indicate your level of agreement on a scale of 1-5:
1 - Strongly disagree
2 - Disagree
3 - Somewhat agree
4 - Agree
5 - Strongly agree
Please motivate your level of agreement where possible.

3.1. (a) Do you agree that the threat of "Malicious Insiders" can be mitigated by the guideline "Control access to PHR data"?

2 - Disagree I found the description of the risk factor / threat at the start of section 2.1 very confusing – specifically the reference to the CSP. I see the malicious insider in the context of this guideline, as someone who is working for the PHR provider, yet the description of the threat refers to the hiring practices of the CSP.

(b) Do you agree that the threat of "Malicious Insiders" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.1 in the background document?

2 - Disagree It may be useful to include a reactive control / mechanism which allows audit logging and analysis to help uncover possible transgressions of employees/insiders (using their valid access rights).

3.2. (a) Do you agree that the threat of "Third-party access" can be mitigated by the guideline "Assess risks involved with third parties"?

4 - Agree No further comments.

(b) Do you agree that the threat of "Third-party access" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.2 in the background document?

4 - Agree No further comments.

3.3. (a) Do you agree that the threat of "Multi-tenancy" can be mitigated by the guideline "Separate customer data"?

Choose an item. No further comments.

(b) Do you agree that the threat of "Multi-tenancy" can be mitigated by employing the control measures as indicated by the ISO controls listed

in Table 2 and as described in the bullet points under section 2.3 in the background document?

4 - Agree No further comments.

3.4. **(a) Do you agree that the threat of "Software intrusions" can be mitigated by the guideline "Prevent malicious code infections"?**

4 - Agree No further comments.

(b) Do you agree that the threat of "Software intrusions" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.4 in the background document?

4 - Agree Consider combining the two bullets as the requirements of the control measures are the same.

3.5. **(a) Do you agree that the threat of "Physical intrusions" can be mitigated by the guideline "Store PHR data in secure data centres"?**

4 - Agree No further comments.

(b) Do you agree that the threat of "Physical intrusions" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.5 in the background document?

4 - Agree No further comments.

3.6. **(a) Do you agree that the threat of "Poor encryption key management" can be mitigated by the guideline "Adopt strong private key management techniques"?**

Choose an item. No further comments.

(b) Do you agree that the threat of "Poor encryption key management" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.6 in the background document?

4 - Agree No further comments.

3.7. **(a) Do you agree that the threat of "Temporary outages" can be mitigated by the guidelines "Ensure business continuity" and "Consider loss of network impact"?**

Choose an item. No further comments.

(b) Do you agree that the threat of "Temporary outages" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.7 in the background document?

4 - Agree No further comments.

3.8. **(a) Do you agree that the threat of "Prolonged and permanent outages" can be mitigated by the guideline "Backup and encrypt PHR data"?**

4 - Agree No further comments.

(b) Do you agree that the threat of “Prolonged and permanent outages” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.8 in the background document?

Choose an item. I am assuming that the first bullet applies to the PHR provider and the second to the CSP?

3.9. (a) Do you agree that the threat of “Data lock-in” can be mitigated by the guideline “Enforce technical interoperability”?

2 - Disagree No further comments.

(b) Do you agree that the threat of “Data lock-in” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.9 in the background document?

2 - Disagree Enforcing technical interoperability but using only one CSP might not sufficiently mitigate the threat. You may need to supplement this with guidance around using a hybrid cloud approach?

3.10. Do you agree that the threat of “Denial of Service (DoS)” can be mitigated by the guideline “Report security incidents?

Choose an item. Reporting alone as a reactive measure is not enough to mitigate for DoS / DDoS / Botnets.

(b) Do you agree that the threat of “Denial of Service (DoS)” can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.10 in the background document?

2 - Disagree There are definitely technical controls (proactive in nature) which the CSP will have to put in place to try and stop these kinds of attacks.

4. Efficacy of the guidelines for secure cloud-based Personal Health Records

4.1. In your opinion, are the guidelines adequate to assist PHR providers in making an informed choice when selecting a cloud service provider to ensure that their customers’ data remains private and secure? Or are there other relevant aspects that need to be considered? Indeed the guidelines will assist PHR providers to make an informed choice when selecting a CSP (based on security aspects). I do, however feel that the guidelines go beyond this and also address the PHR providers’ responsibilities in terms of what security should be in place. Perhaps there is an argument that some of these responsibilities can be performed by either the PHR provider or the CSP. The way the guidelines were presented, however, implies “what all” should be done to mitigate the risks and does not necessarily say “your CSP should have the following in place in order for you to feel comfortable selecting them”.

4.2. Do you think the use of these guidelines by PHR providers will contribute towards more secure cloud-based PHRs? Certainly all controls that are put in place (because PHR providers are implementing the guidelines), will contribute to more secure cloud-based PHRs.

4.3. Do you agree that the different ISO standards used are adequate for the formation of the guidelines? I felt that the ISO27002 could be used to supplement / provide more information about the HOW – see also point 5.3 below. Alternatively it should be made clear that the scope is the WHAT and further details of the HOW can be found in the ISO27002.

5. Overall Impression

5.1. What is your overall opinion of the guidelines? The guidelines provide a useful reference for PHR providers in terms of consolidating the controls / measures that are required to secure cloud-based PHRs.

5.2. Can you recommend any way in which the guidelines can be improved? Some comments were provided earlier about possibly structuring the guidelines differently to improve usability. In addition, I think you can check that the controls from the different standards are collated where relevant. For example, section 2.4 presents two actions (bullets) based on two standards. These essentially address the same thing thus could be one statement / action referencing both standards. This was also mentioned in section 3.3 (b). Also check this for all the other guidelines.

5.3. Please provide any final comments, criticism or suggestions. The guidelines focus a lot on WHAT and not HOW. Indeed, the scope of this project may have been on the WHAT and not the HOW. However, consider that the ISO27002 (according to which the ISO27799 is structured), does provide a lot of the HOW detail and thus your PHR provider should also be applying the guidance provided within the ISO27002. Refer to 10.4.1 in ISO27002 (related to 7.7.4.1 in ISO27799) as an example. This (ISO27002) would be applicable to all the guidelines from ISO27799.

Thank you for your input regarding the guidelines for secure cloud-based Personal Health Records. Your contribution will provide valuable insight into their value as an output for this research, as well as allow the guidelines to be further improved.

Please save and submit this document via e-mail at: s209029505@live.nmmu.ac.za

Nelson Mandela Metropolitan University

for tomorrow

Elite Interview Questionnaire on Guidelines for secure cloud-based Personal Health Records

The purpose of this questionnaire is to obtain expert perspectives and feedback on the utility, quality, efficacy and overall impression of the guidelines for secure cloud-based Personal Health Records (PHRs) as described in the background document provided to you. If you have any queries concerning the questionnaire, you can contact me at: 209029505@live.nmmu.ac.za

Please refer to Table 2 and the discussion of the guidelines as provided in the background document before completing this questionnaire.

1. Reviewer Demographics

Please provide the following details about yourself:

1.1. Title and full name:

1.2. What is your current job title? Researcher

1.3. What are your areas of expertise? Cloud Computing, Information Security and Health Information Systems

1.4. How many years' experience do you have in the field of Cloud Computing 5

1.5. Please indicate your level of knowledge in the field of Cloud Computing (4) Very knowledgeable

1.6. How many years' experience do you have in the field of Health Informatics (for example Personal Health Records)? 5

1.7. Please indicate your level of knowledge in the field of Health Informatics (for example Personal Health Records) (3) Knowledgeable

1.8. How many years' experience do you have in the field of Information Security? 5

1.9. Please indicate your level of knowledge in the field of Information Security (4) Very knowledgeable

1.10. Please provide any further information related to your professional status and any knowledge levels that you feel are relevant to this review process. Click here to enter text.

2. Utility of the guidelines for secure cloud-based Personal Health Records

2.1. Was the information provided in the document sufficient for a clear understanding of the need and function of the proposed guidelines? The document is somehow sufficient with the exception of “Physical Intrusion”. The PHR providers who are consumers of PaaS have limited control over the physical location of their hosted services. This guideline would be more relevant to IaaS providers and IaaS consumers. Instead, PHR providers may need to ensure that this is taken care of in the SLA.

2.2. Was the description of the guidelines and control measures proposed to address the risks associated with cloud-based PHRs clear and easily understood? Yes they are clear with the exception of Multi-tanancy. Separation of development, test and production facilities has nothing to do with multi-tenancy. Multi-tenancy can still be an issue in production facilities if there implementation flaws. A different solution may be required.

2.3. Can these guidelines be easily understood and utilized by PHR providers to make an informed choice when selecting a cloud service provider to ensure that their customers’ data is kept private and secure? Yes they can be understood and utilized with the exception of physical intrusion and multi-tanancy as commented above.

2.4. Do you think these guidelines will be useful/ beneficial to PHR providers? Please elaborate on your answer. They will be very useful and beneficial. How ever, the guidelines may still be improved by considering threats that are more current such as the “The Treacherous 12 - CSA’s Cloud Computing Top Threats in 2016” and “An analysis of security issues for cloud computing” by Hashizume et al (2013). The threats considered here were published some 4-5 years back. If guidelines of more recently published threats like the example above, it would be more beneficial.

3. Quality of the guidelines for secure cloud-based Personal Health Records

For each of the questions below please indicate your level of agreement on a scale of 1-5:

1 - Strongly disagree
2 - Disagree
3 - Somewhat agree
4 - Agree
5 - Strongly agree

Please motivate your level of agreement where possible.

3.1. (a) Do you agree that the threat of "Malicious Insiders" can be mitigated by the guideline "Control access to PHR data"?

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Malicious Insiders" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.1 in the background document?

4 - Agree Click here to enter text.

3.2. (a) Do you agree that the threat of "Third-party access" can be mitigated by the guideline "**Assess risks involved with third parties**"?

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Third-party access" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.2 in the background document?

4 - Agree Click here to enter text.

3.3. (a) Do you agree that the threat of "Multi-tenancy" can be mitigated by the guideline "Separate customer data"?

2 - Disagree See my comments on multi-tenancy above.

(b) Do you agree that the threat of "Multi-tenancy" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.3 in the background document?

2 - Disagree Multi-tenancy as a property of the cloud is not an issue but threats associated with it are. Measures that address such threats are more desirable than taking away multi-tenancy. Having dedicated resources should be more more expensive hence taking away the cost benefit.

3.4. (a) Do you agree that the threat of "Software intrusions" can be mitigated by the guideline "Prevent malicious code infections"?

Choose an item. Click here to enter text.

(b) Do you agree that the threat of "Software intrusions" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.4 in the background document?

4 - Agree Click here to enter text.

3.5. (a) Do you agree that the threat of "Physical intrusions" can be mitigated by the guideline "Store PHR data in secure data centres"?

2 - Disagree PHR prioviders have no control over physical data centers (IaaS).

(b) Do you agree that the threat of "Physical intrusions" can be mitigated by employing the control measures as indicated by the ISO

controls listed in Table 2 and as described in the bullet points under section 2.5 in the background document?

2 - Disagree It can be mitigated but the PHR provider has limited/no control over IaaS.

3.6. **(a) Do you agree that the threat of "Poor encryption key management" can be mitigated by the guideline "Adopt strong private key management techniques"?**

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Poor encryption key management" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.6 in the background document?

4 - Agree Click here to enter text.

3.7. **(a) Do you agree that the threat of "Temporary outages" can be mitigated by the guidelines "Ensure business continuity" and "Consider loss of network impact"?**

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Temporary outages" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.7 in the background document?

4 - Agree Click here to enter text.

3.8. **(a) Do you agree that the threat of "Prolonged and permanent outages" can be mitigated by the guideline "Backup and encrypt PHR data"?**

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Prolonged and permanent outages" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.8 in the background document?

4 - Agree Click here to enter text.

3.9. **(a) Do you agree that the threat of "Data lock-in" can be mitigated by the guideline "Enforce technical interoperability"?**

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Data lock-in" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.9 in the background document?

4 - Agree Click here to enter text.

3.10. **Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by the guideline "Report security incidents?**

4 - Agree Click here to enter text.

(b) Do you agree that the threat of "Denial of Service (DoS)" can be mitigated by employing the control measures as indicated by the ISO controls listed in Table 2 and as described in the bullet points under section 2.10 in the background document?

3 - Somewhat agree Click here to enter text.

4. Efficacy of the guidelines for secure cloud-based Personal Health Records

4.1. **In your opinion, are the guidelines adequate to assist PHR providers in making an informed choice when selecting a cloud service provider to ensure that their customers' data remains private and secure? Or are there other relevant aspects that need to be considered?** The guidelines are adequate. They can however still be improved by considering more recent threats in the cloud as published by the CSA.

4.2. **Do you think the use of these guidelines by PHR providers will contribute towards more secure cloud-based PHRs?** yes, definitely

4.3. **Do you agree that the different ISO standards used are adequate for the formation of the guidelines?** Yes they are adequate and current.

5. Overall Impression

5.1. **What is your overall opinion of the guidelines?** These guidelines are indeed a great initiative.

5.2. **Can you recommend any way in which the guidelines can be improved?** As stated in earlier comments, it can still be improved by considering more recent threats as published by the CSA. Threats considered in the current guidelines were mostly published in 2011-2012 when the cloud was still in its early stages and some are indeed still prevalent to this day.

5.3. **Please provide any final comments, criticism or suggestions.** Most of my criticism and suggestions are as stated in the earlier sections of this questionnaire. But mainly, it is the physical intrusion and multi-tenancy that need to be reconsidered. And lastly, to also consider more current literature on threats in the cloud.

Thank you for your input regarding the guidelines for secure cloud-based Personal Health Records. Your contribution will provide valuable insight into their value as an output for this research, as well as allow the guidelines to be further improved.

Please save and submit this document via e-mail at: s209029505@live.nmmu.ac.za

APPENDIX E – Proofreader certificate

Language Quality Assurance Practitioners

Mrs KA Goldstone

Dr PJS Goldstone

14 Erasmus Drive
Summerstrand
Port Elizabeth
6001
South Africa

Tel/ Fax: +27 41 583 2882

Cell: +27 73 006 6559

Email: kate@pemail.co.za

pat@pemail.co.za

26 May 2016

TO WHOM IT MAY CONCERN

We hereby certify that we have language-edited the dissertation of Avuya Mxoli entitled: GUIDELINES FOR SECURE CLOUD-BASED PERSONAL HEALTH RECORDS.

We are satisfied that, provided the changes we have made are effected to the text, the language is of an acceptable standard, and is fit for publication.

KA Goldstone

Kate Goldstone

BA (Rhodes)

SATI No: 1000168

UPE Language Practitioner (1975-2004)

NMMU Language Practitioner (2005)

PJS Goldstone

Dr Patrick Goldstone

BSc (Stell.)

DEd (UPE)