



Department of Computing Sciences

A Hybrid Model for Managing Personal Health Records in South Africa

Michael Kyazze

Supervisor: Prof JL Wesson

Co-Supervisor: Dr Kevin Naudé

Department of Computing Sciences

December 2014

Submitted in fulfilment of the requirements for the degree of
Magister Scientiae in the Faculty of Science at the Nelson Mandela Metropolitan University

Declaration

I, Michael Kyazze, hereby declare that the dissertation for the degree Magister Scientiae is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

Michael Kyazze

A handwritten signature in black ink, appearing to read "Michael Kyazze", is placed over a light grey rectangular background.

Acknowledgements

I would like to thank my supervisors, Prof Janet Wesson and Dr Kevin Naudé, for their invaluable guidance and continuous support for the duration of this research. I wish to express my gratitude for the many hours that were spent reading through this document and the suggestions that were made to improve the content and structure. I would like to thank them for their encouragement.

I would also like to thank those that played a part in assisting me with the completion of this dissertation:

- Sr. Antoinette Goosen, Deputy director NMMU Campus Health Service
- Mr Ross Chamber, Medical Secretary and Basic Ambulance Assistant NMMU Campus Health Service
- Miss Eva Ssozi for proof reading this dissertation
- My family and friends whose continued support and confidence helped me complete this work

I would also like to thank the Department of Computing Sciences for enabling me to conduct my research through the resources they provided. I appreciate the support that enabled me to present my work at the 2014 Global Telehealth conference held in Durban and the Interact 2013 African Masters Symposium held in Cape Town.

I would especially like to thank the NMMU Centre of Excellence programme for providing the necessary finance for this research study.

Summary

Doctors can experience difficulty in accessing medical information of new patients. One reason for this is that the management of medical records is mostly institution-centred. The lack of access to medical information may negatively affect patients in several ways. These include new medical tests that may need to be carried out at a cost to the patient and doctors prescribing drugs to which the patient is allergic. This research investigates how patients can play an active role in sharing their personal health records (PHRs) with doctors located in geographically separate areas.

In order to achieve the goal of this research, existing literature concerning medical health records and standards was reviewed. A literature review of techniques that can be used to ensure privacy of health information was also undertaken. Interview studies were carried out with three medical practices in Port Elizabeth with the aim of contextualising the findings from the literature study.

The Design Science Research methodology was used for this research. A Hybrid Model for Managing Personal Health Records in South Africa is proposed. This model allows patients to view their PHRs on their mobile phones and medical practitioners to manage the patients' PHRs using a web-based application. The patients' PHR information is stored both on a cloud server and on mobile devices hence the hybrid nature. Two prototypes were developed as a proof of concept; a mobile application for the patients and a web-based application for the medical practitioners. A field study was carried out with the NMMU health services department and 12 participants over a period of two weeks.

The results of the field study were highly positive. The successful evaluation of the prototypes provides empirical evidence that the proposed model brings us closer to the realisation of ubiquitous access to PHRS in South Africa.

Keywords: personal health records, ubiquitous access, cloud storage, MongoDB, hybrid model, Encryption

Table of Contents

Declaration	i
Acknowledgements	ii
Summary	iii
Table of Contents	iv
List of Figures	viii
List of Tables	ix
List of Abbreviations	x
Chapter 1: Introduction.....	1
1.1 Background	1
1.2 Project Relevance	3
1.3 Problem statement	3
1.4 Aim of Research:.....	3
1.5 Research objectives	4
1.6 Research Questions	4
1.7 Research Methods	5
1.8 Possible limitations	7
1.9 Ethical considerations	7
1.10 Scope and Constraints	7
1.11 Conclusion and Dissertation Structure	7
Chapter 2: Personal Health Information Management	9
2.1 Introduction	9
2.2 Personal Health Information	9
2.2.1 Paper vs. Electronic Health Data	9
2.2.2 Electronic Health	11
2.3 Privacy Concerns and Security Mechanisms	14
2.3.1 CIA Triad Model.....	16
2.3.2 Overview of information security concepts	17
2.3.3 Applying the CIA Model to Personal Health Records.....	18
2.4 Legislation and guidelines.....	24
2.4.1 US Guidelines	24

2.4.2	South African Legislation	24
2.5	Personal Health Records	25
2.5.1	Overview and Benefits.....	26
2.5.2	Data Encoding Standards.....	27
2.5.3	PHR Use Cases	29
2.6	Personal Health Records Requirements	31
2.6.1	Functional Requirements	31
2.6.2	Data Requirements.....	31
2.6.3	Security and Privacy Guidelines.....	33
2.7	Conclusion.....	34
Chapter 3:	Mobile Health Applications and Architectures.....	36
3.1	Introduction	36
3.2	Mobile Devices in HealthCare	37
3.2.1	Classification of mHealth Applications	38
3.2.2	Motivation for personal health information management	39
3.3	PHR categories.....	40
3.4	PHR Evaluation Criteria.....	41
3.5	Review of Existing Applications.....	43
3.5.1	Microsoft Health Vault (MHV)	43
3.5.2	HealthSpek	44
3.5.3	Capzule PHR.....	46
3.5.4	In Case of Emergency (ICE).....	47
3.5.5	Summary	47
3.6	Analysis of existing applications.....	48
3.7	Existing PHR architectures	50
3.7.1	Connectivity Coverage.....	52
3.7.2	Ubiquitous Technology Baseline	53
3.8	Conclusion.....	57
Chapter 4:	Hybrid PHR Management Model.....	59
4.1	Introduction	59
4.2	Interview Studies.....	60
4.2.1	Medical Practice A.....	60

4.2.2	Medical Practice B	61
4.2.3	Student Medical Centre.....	62
4.2.4	Summary of findings.....	63
4.3	Model Design	63
4.3.1	Hybrid PHR Architecture	63
4.3.2	Encryption Approach Used.....	63
4.3.3	Hybrid PHR Management Model.....	65
4.4	System Design.....	68
4.4.1	Functional Design	68
4.4.2	Data Design.....	69
4.4.3	Interface Design	71
4.5	Implementation.....	74
4.5.1	Implementation tools	74
4.5.2	Mobile Application	80
4.5.3	Web Application	81
4.6	Expert Review	81
4.7	Conclusion.....	82
Chapter 5:	Evaluation	83
5.1	Introduction	83
5.2	Evaluation Design	83
5.2.1	Evaluation Objectives	84
5.2.2	Participants.....	84
5.3	Field Study Design.....	86
5.3.1	Evaluation Metrics	87
5.3.2	Evaluation Instruments	87
5.4	Field Study Evaluation Results	88
5.4.1	Performance Results	88
5.4.2	User Satisfaction Results	92
5.4.3	Discussion.....	100
5.5	Design Implications.....	101
5.6	Conclusions	102
Chapter 6:	Conclusion	103

6.1	Introduction	103
6.2	Achievements of Research Objectives	103
6.3	Reflections on the HNSF.....	104
6.4	Research Contributions	105
6.4.1	Theoretical Contributions	105
6.4.2	Practical Contributions.....	106
6.5	Limitations	106
6.6	Future Research.....	107
	References.....	108
	Appendices.....	118
	Appendix A: Ethics Clearance Letter	118
	Appendix B: HIPAA Technical safeguards	119
	Appendix C: PHR Functional requirements	120
	Appendix D: Application Process Flow Diagrams.....	122
	Appendix E: Patient Tasks.....	124
	Appendix F: Medical Practice Tasks	125
	Appendix G: Participant Consent Forms	126
	Appendix H: Research Publication and Award	129
	1. 2014 Global Tele-health Conference Paper Presentation.....	129
	2. Best Presentation at the 2013 Interact African Masters Consortium.....	132
	Appendix I: Patient After-Scenario Questionnaire	133
	Appendix J: Patient Post-Test Questionnaire	136
	Appendix K: Medical Practice After-Scenario Questionnaire.....	138
	Appendix L: Medical Practice Post-Test Questionnaire.....	140
	Appendix M: Patient and Medical Practice Interaction Diagram.....	142

List of Figures

Figure 1-1: Design Science Research Process, adapted from (Peppers et al., 2006)	6
Figure 2-1: CIA Triad Model, adapted from (Solomon & Chapple, 2005)	16
Figure 2-2: Hierarchical structure of medical records (Benaloh <i>et al.</i> , 2009)	20
Figure 2-3: Standard Overview, adapted from (Donald T, 2010).....	28
Figure 2-4: Create and Maintain Access Control Lists, adapted from (US.DoH, 2007).....	30
Figure 2-5: A sample PHR by Microsoft Health Vault, adapted from (MSHV, 2013).....	33
Figure 2-6: PHR model privacy notice (HealthIT.gov, 2008)	34
Figure 3-1: Illustration of mHealth design space, adapted from (Klasnja & Pratt, 2012).....	38
Figure 3-2: Necessity for personal health information management.....	39
Figure 3-3:Microsoft health vault Platform Overview (Microsoft, 2013)	43
Figure 3-4: Sample HealthSpek Patient Profile (HealthSpek, 2013).....	45
Figure 3-5: Doctor access website (HealthSpek, 2013).....	45
Figure 3-6: Sample PHR from the Capzule mobile application	46
Figure 3-7: Sample PHR from the ICE mobile application.....	47
Figure 3-8: Hybrid Architecture, adapted from (Steele & Lo, 2012)	53
Figure 3-9: Cloud-Based PHR System Architecture (Gorp& Comuzzi, 2012).....	55
Figure 3-10: Three tier architecture, adapted from (Helal <i>et al.</i> , 2001).....	56
Figure 4-1: Ciphertext Policy Attribute Based Encryption (Bethencourt <i>et al.</i> , 2007)	64
Figure 4-2: Proposed Adaptation of the Hybrid PHR Architecture.....	66
Figure 4-3: Use case diagram for PHRs	68
Figure 4-4: PHR UML Class Diagram	70
Figure 4-5: Login and Home Screens	71
Figure 4-6: Search Results and Permissions Screen.....	72
Figure 4-7: A sample list of patients connected to a medical practice	73
Figure 4-8: Sample patient chart.....	73
Figure 4-9: Cloud computing, adapted from (Chun, 2012)	75
Figure 5-1: Patient Task Success (n=12)	89
Figure 5-2: Encryption Performance (n=12).....	91
Figure 5-3: Adding health information to the mobile application (n=12)	93
Figure 5-4: Ease of Use, Usefulness, Ease of Learning and Satisfaction (n=12)	94
Figure 5-5: Overall Satisfaction (NMMU Health Services).....	95
Figure 5-6: Searching for patients on the system.....	96
Figure 5-7: Viewing a patient's self-reported data	97
Figure 5-8: Adding a patient's consultation data (NMMU Health Services)	98

List of Tables

Table 2-1: Paper Vs. Electronic Health Data, adapted from (Bakker, 2006)	10
Table 2-2: Comparison of EMR, EHR and PHR functionality , adapted from (Caligtan & Dykes, 2011)	13
Table 2-3: PHR Data requirements, adapted from (AHIMA, 2013)	32
Table 3-1: Criteria for PHR evaluation (Kim & Johnson, 2002).....	42
Table 3-2: Compliance of PHR applications with the evaluation criteria (HealthSpek, 2013; Microsoft, 2013)	48
Table 3-3: Classification of PHR architectures based on Connectivity and Technology (Steele & Lo, 2012).....	51
Table 4-1: Desired features of a PHR cloud storage service	76
Table 4-2: Core NoSQL Systems, adapted from (Stefan, 2013; Tudorica & Bucur, 2011).....	78
Table 4-3: Functionality of MongoDB and CouchDB (Apache, 2005; MongoDB, 2009)	79
Table 5-1: Participant experience with Android phones (n=12).....	85
Table 5-2: Gender of Participants (n=12)	85
Table 5-3: Mean, Standard Deviation and Median rating of patient tasks (n=12)	93
Table 5-4: Feedback from patient participants	98
Table 5-5: Feedback from NMMU Health Services.....	99

List of Abbreviations

ASQ	After Scenario Questionnaire
CIA	Confidentiality Integrity Availability
CSIR	Council for Scientific and Industrial Research
DSR	Design Science Research
DSRM	Design Science Research Methodology
ICT	Information Communication Technology
EMR	Electronic Medical Record
EHR	Electronic Health Record
HNSF	National Health Normative Standards Framework for Interoperability in eHealth in South Africa
PHR	Personal Health Record
HIPPA	The Health Insurance Portability and Accountability Act of 1996 (USA)
UML	Unified Modelling Language
CP-ABE	CipherText Policy Attribute Based Encryption
NMMU	Nelson Mandela Metropolitan University
NDOH	National Department of Health (South Africa)

Chapter 1: Introduction

1.1 Background

Doctors can experience difficulty in accessing historical medical information of new patients since the management of their electronic medical records (EMRs) is mostly institution-centred. That is, medical care providers often do not share EMRs amongst themselves (Endsley, Kibbe, Linares, & Colorafi, 2006; Steele & Min, 2010). One way to address this is through the use of Personal Health Records (PHRs). A PHR provides a summary of an individual's medical history; it is initiated and managed by the individual (Endsley et al., 2006; Garets & Davis, 2006). The information contained in PHRs can be beneficial for keeping track of health related issues, easy sharing with medical personnel, and proper travel planning. In case of an emergency while travelling, foreign medical providers who are not familiar with a new patient could easily gain access to the individual's health record.

The majority of the South African population, especially in rural areas, have inadequate access to basic healthcare services. This may lead to increased medical errors, delays of patient referrals and long queues of patients in hospitals (Coleman Alfred, 2010). The usage of information and communications technology (ICT) in the health sector is defined as eHealth (Rizo, Enkin, Jadad, & Oh, 2005) and can be leveraged in order to improve health service delivery in South Africa.

Research on the integration of eHealth into the South African National Health system is required to strengthen its effectiveness (Mayosi et al., 2011). To meet this need, formal postgraduate Health Informatics programmes have been developed at the University of KwaZulu-Natal, the Walter Sisulu University and at the University of South Africa (Mars & Seebregts, 2008). The programmes offered at the above institutions are focused on generating research output in eHealth and Telemedicine (providing clinical care at a distance). Whilst this partly addresses the research needs of the South African Health system, ongoing research does not explicitly address how mobile devices can be utilised in the health sector. More research is needed to bridge this gap.

The pervasive nature of mobile devices makes them an ideal tool for capturing, measuring and monitoring an individual's health and well-being. Mobile devices can be used to facilitate ubiquitous access to PHRs. The provision of health-related services via mobile communications is defined as mHealth and can help in bringing health services closer to

individuals without access to standard desktop computers (Vital Wave Consulting, 2009). Several mobile health (mHealth) interventions and applications have been implemented, some of which address the problem of inadequate access to medical information (Klasnja & Pratt, 2012). Personal health information management refers to the ability to access health information from anywhere, and usage of contextual information with health information could benefit from mobile-based solutions. For example, a mobile device can be used to measure the impact of an individual's exercise plan and the effects on their weight over a given period of time (Klasnja & Pratt, 2012).

Several mHealth interventions focusing on the accessibility of PHRs have been designed and implemented. Most of such initiatives are specific to the developer's geographical location and are tailored for their local medical data legislation and requirements. For example, Microsoft Health Vault (MHV) is a prominent PHR platform that categorises users and applies legislation depending on their geographical regions (United States, Canada, France, European Union and others). This further highlights the importance of complying with local legislation when managing PHRs.

There is an increase in the usage of mobile phones as platforms for the delivery of health interventions (Klasnja & Pratt, 2012). The increase means that a growing number of individuals will be able to access their health records ubiquitously in the future. However, little attention has been given to the implementation and evaluation of the proposed designs to determine their effectiveness and potential usefulness in South Africa (Mars & Seebregts, 2008; Mxoli, Mostert-Phipps, & Gerber, 2014). The existing models for EHRs and PHRs do not explicitly address the challenges of using mobile devices to manage PHRs. These challenges include the limited screen space and the need for cloud backup and storage in order to facilitate ubiquitous access and sharing of information. There is a need to propose or extend existing models to the mobile space.

The main objective of this study is to design a model that can facilitate ubiquitous management and secure sharing of PHRs in South Africa. A literature study was carried out to gain a better understanding of PHRs and how ubiquitous access to PHRs can be achieved. The study covered security mechanisms that can be used to ensure patient confidentiality and existing PHR applications and architectures. The findings from the literature study provided part of the requirements for the proposed PHR Model. Interview studies were

carried out with three medical practices in Port Elizabeth. The interview studies helped to contextualise the requirements identified from the literature reviews.

A hybrid PHR Model was designed and two prototype applications were then implemented as a proof of concept. One prototype application was designed for patients and the other for medical care providers. A paper discussing the design and implementation of the prototype applications was presented at the 2014 Global Telehealth Conference (Kyazze, Wesson, & Naude, 2014).

A two-week field study was carried with the NMMU health services department and 12 patient participants. The prototype applications were rated positively by the participants.

1.2 Project Relevance

An individual's personal health information is beneficial only if they can access it whenever they need to. This could be when visiting a different health service provider who has no access to their medical history. Ubiquitous access to health data can save users from costs, which may be incurred in repeating medical tests, which have already been performed. However, individuals may have concerns about the privacy of their health information. Individuals may trust healthcare providers with their health information, but they may be sceptical about storing the same information with a third party storage service. Security mechanisms as well as privacy measures that aim to address such concerns are discussed. Mobile devices are used as one of the means of providing ubiquitous access to the information.

1.3 Problem statement

There is a lack of ubiquitous and secure access to PHRs in South Africa.

1.4 Aim of Research:

The aim of this research is to propose a model to facilitate ubiquitous access and secure sharing of PHRs using mobile devices in South Africa.

1.5 Research objectives

The main objective of this research is:

To develop a model to facilitate ubiquitous access and secure sharing of PHRs in South Africa.

The following sub-objectives will support achieving the main research objective:

- (i) To identify requirements for ubiquitous management of PHRs and existing user concerns that may hinder PHR adoption (Chapter 2).
- (ii) To review existing mHealth systems and architectures that can be used to support ubiquitous access and secure sharing of PHRs (Chapter 3).
- (iii) To design a model to facilitate ubiquitous access and secure sharing of PHRs and implement a prototype to validate the proposed model (Chapter 4).
- (iv) To evaluate the effectiveness and usefulness of the prototype applications (Chapter 5).

1.6 Research Questions

The primary research question for this project is:

How can PHRs be effectively managed and shared securely using mobile devices?

In order to address the primary research question, the following sub-questions are also answered. The research questions below are formulated to achieve the research objectives.

- (i) **RQ1:** What are the requirements for ubiquitous access of PHRs?
- (ii) **RQ2:** What are the strengths and shortcomings of existing mHealth Systems that can be used to support the management of PHRs?
- (iii) **RQ3:** How can a model be designed and prototype applications implemented to support personal health management?
- (iv) **RQ4:** How usable and effective are the prototypes designed to validate the proposed model?

1.7 Research Methods

Research methods refer to the plan which guide a researcher in achieving the aims of the research and answering the associated research questions (Hofstee, 2011). This section discusses the logical structure of how this research was carried out as well as the methods that were used to address each of the research questions.

This research used the Design Science Research (DSR) methodology. DSR integrates the design and development phase with the research process and this leads to an artefact that can adequately answer the research questions. DSR has a relevance cycle that ensures that the requirements are met and a rigor cycle which ensures that a solid theory base underpins the research (Ellis & Levy, 2010). DSR was chosen over the positivism philosophy, which does not have explicit guidelines on how an artefact should be developed but emphasises that only observable phenomena should lead to the production of credible data in the natural sciences (Saunders, Lewis, & Thornhill, 2009).

DSR should be goal-centred (Ellis & Levy, 2010). The goal of this study is to produce a model to facilitate ubiquitous access and secure sharing of PHRs.

Peppers *et al* (2006) present a conceptual Design Science Research process model (DSRP) consisting of six activities: *problem identification and motivation; objectives of a solution; design and development; demonstration; evaluation and communication.*

The DSRP aims to provide Design Science (DS) researchers with a mental model for what parts of DS research output may look like. Offermann & Platz (2009) provide an approach to design research in the area of information systems. The DSRP is divided into phases that consist of steps to which one may refer. Whilst both approaches highlight the same processes, the DSRP was chosen for this research because its activities could easily be mapped onto the research questions. The mapping is illustrated in Figure 1-1.

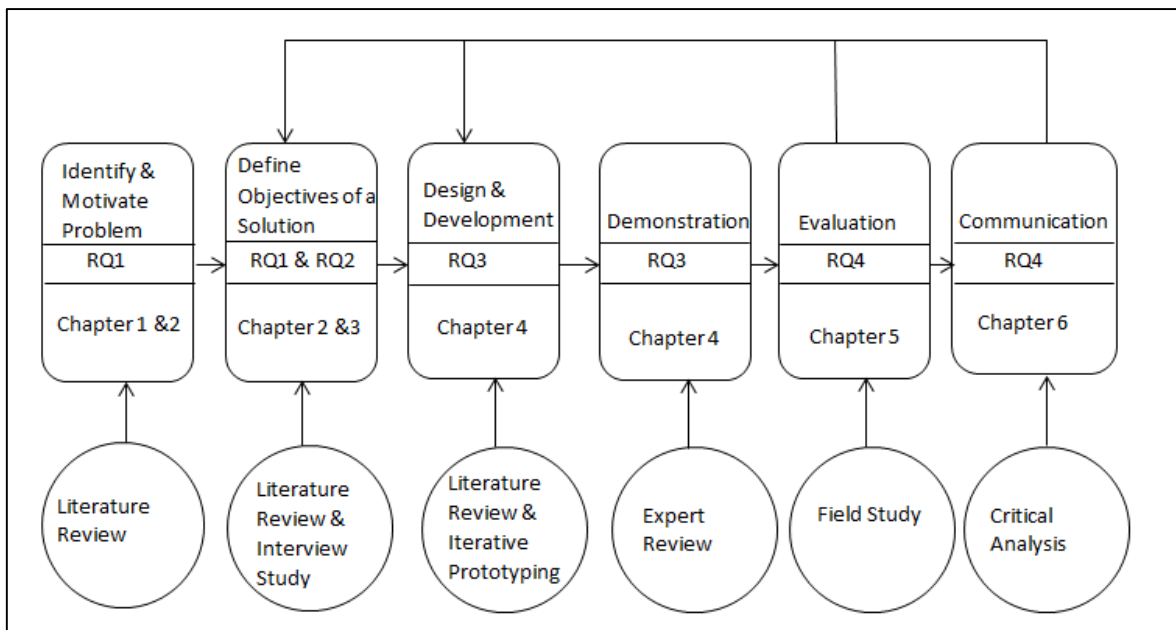


Figure 1-1: Design Science Research Process, adapted from (Peffers et al., 2006)

Problem identification and motivation: The goal of this research is to develop a model to enable individuals to ubiquitously access and manage their PHRs. The problem was identified through a literature study.

Objectives of a solution: An ideal solution should infer its objectives from the problem definition (Peffers et al., 2006). A literature review was carried out to identify the shortcomings of current offerings, and to motivate objectives for the proposed solution.

Design and development: Literature was reviewed in order to gain a better understanding of existing models and designs. The synthesis resulted in a new conceptual model, which was validated by implementing two prototype applications.

Demonstration: The prototype applications were demonstrated to expert users and the feedback incorporated into the design before a field study was conducted.

Evaluation: The prototypes were evaluated to determine if they could facilitate ubiquitous access and management of PHRs. A two-week field study was carried out with the NMMU health services department and patient participants. Performance and user satisfaction data was collected and discussed (chapter 5).

Communication: The literature review findings were presented at the 2013 INTERACT African Masters Consortium. The INTERACT presentation was voted as the best

presentation at the Masters symposium. The award (certificate) can be viewed in Appendix H.

A paper discussing the design and implementation of the prototype applications was presented at the 2014 Global Telehealth Conference. The conference proceedings were published by iOS press in the Studies in Health Technology and Informatics journal (Kyazze *et al.*, 2014).

Hevner *et al.* (2004) provide a set of seven guidelines with the purpose of assisting researchers, reviewers, editors, and readers to understand the requirements of DSR. These guidelines were used throughout the research process to ensure that the deliverables of each phase are rigorous, have utility and are of high quality.

1.8 Possible limitations

The proposed model uses a hybrid, centralised cloud storage service. Future work can adapt the model to support distributed cloud storage. This could be useful for medical practices, which may have reservations about using centralised cloud storage. One of the limitations of centralised cloud storage is that if the data is corrupted, the medical practices may lose their data.

1.9 Ethical considerations

Ethical clearance was obtained in order to carry out the field study discussed in Chapter 5. The ethics clearance letter is included in Appendix A.

1.10 Scope and Constraints

The field study was limited to one medical care provider (NMMU Health Services). Future work can involve carrying out a field study involving more than one medical practice.

The research does not include Electronic Health Records (EHRs) or Electronic Medical Records (EMRs), which are managed by the Care Delivery Organisations (CDOs).

1.11 Conclusion and Dissertation Structure

This dissertation is comprised of six chapters, each of which aims to achieve a specific research objective. This section gives a brief overview of each chapter.

Chapter 1 (Introduction) provided a background on problems associated with trying to access PHRs. The motivation for this research was also provided. Concepts related to the topic were introduced. The problem statement, aims of the research, research questions and objectives of the research were addressed. The scope and constraints were then identified. The research methodology of this study was discussed in detail. The chapter concludes with the envisaged contributions of this research.

The literature study is covered in Chapters 2 and 3. Chapter 2 introduces and discusses personal health information management in detail. PHR standards and Legislation are reviewed. Mechanisms that can be used to secure PHRs are also discussed. Chapter 2 concludes with the identification of PHR requirements for South Africa.

Mobile health applications and architectures are discussed in Chapter 3. Current systems that facilitate mobile management of health records are reviewed. Chapter 3 concludes by identifying a suitable PHR architecture for South Africa.

Chapter 4 (Design and Implementation) presents the Hybrid PHR Management Model. The model is designed using knowledge obtained from the literature studies and interview studies with medical practices in Port Elizabeth. Chapter 4 also presents the design and implementation of two prototype applications as a proof of concept of the proposed model.

Chapter 5 (Evaluation and Results) discusses the results of a two-week field study carried out with the NMMU health services department and 12 patient participants.

Chapter 6 (Conclusions and Recommendations) discusses conclusions drawn from this research. The chapter verifies that the outlined objectives were achieved and presents ideas for future research.

Chapter 2: Personal Health Information Management

2.1 Introduction

Chapter One identified the lack of a model for ubiquitous management of PHRs in South Africa. The research problem and research objectives were also stated. The first phase of the Design Science Research Methodology (DSRM) is the problem identification and motivation phase. This chapter completes the first phase of the DSRM by further investigating the problem domain. The objective of this chapter is to identify requirements for managing and securely sharing PHRs in South Africa. This is achieved by reviewing existing literature to gain a comprehensive understanding of electronic health information management, the privacy and security issues associated with PHRs and how individuals can take an active role in the management of their health information. In so doing, the chapter addresses part of research question 1: *What are the requirements for ubiquitous access of Personal Health Records (PHRs)?*

2.2 Personal Health Information

Section 2.2.1 compares paper and electronic health data with the aim of highlighting the benefits of electronic health data. A classification of electronic health data is presented in section 2.2.2, which include Electronic Medical Record (EMR), Electronic Health Record (EHR) and Personal Health Record (PHR). The section concludes with a comparison of the key information they contain.

2.2.1 Paper vs. Electronic Health Data

The availability of electronic health data in general and EHRs in particular have a significant impact on healthcare (Bakker, 2006). This is because they enable continuity of care by providing health care professionals with historical health information on patients. It is important to understand the current evolution of health records from paper based to electronic versions in order to aid the design of better eHealth systems. This is discussed in the form of a comparison between the two.

Table 2-1: Paper Vs. Electronic Health Data, adapted from (Bakker, 2006)

Paper Records	Electronic Health Data
They can only be viewed at one location at any given time (where the physical document is present).	They can be viewed from any number of locations at the same time.
Access to the records is either permitted or not (yes or no).	The authorisation of the reader determines which part of the data will be presented.
It is in generally impossible to record who has seen the data and when.	It is possible, in principle to keep a trail of the use.

Table 2-1 shows some of the differences between paper and electronic records. Electronic health data makes it easier to introduce new forms of health care delivery since care can easily be spread over distributed health facilities. More benefits of electronic health data are highlighted below (Bakker, 2006).

Benefits of Electronic Health Data

- (i) Data about the medical history of the patients and their current situation can be reorganised and presented chronologically, or by the grouping of relevant details and events.
- (ii) The medical record is no longer restricted to the data recorded from single or disparate providers.
- (iii) Protocols and guidelines can support the decision-making processes of healthcare professionals.
- (iv) Medical data access rules can be made explicit, and auditing of access is possible.

The stated benefits highlight the significance of electronic health data in relation to paper-based medical records. However, these benefits can only be achieved with a proper understanding of the format of medical health data. There is therefore, a need to gain an understanding of electronic health data and how it is currently structured and classified by other researchers and medical practitioners. The next section introduces the concept of Electronic Health and defines related terminologies.

2.2.2 Electronic Health

Eysenbach, (2001) defines eHealth as an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. Kwankam, (2004) defines eHealth as an all-encompassing term for the combined use of electronic information and communication technology (ICT) for clinical, educational, research and administrative purposes in the health sector. A systematic review of 51 unique published definitions of eHealth carried out by Rizo *et al.*, (2005) noted that the precise meaning varied with the context in which the eHealth term was used, and recognised the difficulty of finding a universally acceptable and applicable formal definition. Whilst there are many offered definitions of eHealth, most of them highlight the focus on the use of ICT in the health sector, hence the definition used for the purposes of this research is:

The usage of ICT in the health sector with an aim of improving service delivery is known as eHealth (Rizo et al., 2005).

Open Clinical, (2011) identifies the key application areas of eHealth as:

- (i) Electronic Health Information.
- (ii) Telemedicine and telecare services; health information networks.
- (iii) Decision support tools.
- (iv) Internet-based technologies and services.

The key application areas of Electronic Health Information and Internet-based technologies services are the emphasis of this research. Specifically the usage of Internet-based technologies in supporting access to Electronic Health Information.

Electronic health information is classified as Electronic Medical Records (EMRs), Electronic Health Records (EHRs), or Personal Health Records (PHRs). The terms EMR and EHR are often used interchangeably, however they describe completely different concepts (Garets & Davis, 2006). The definitions used for the purposes of this research are given below to ensure universality in understanding of these terms:

An Electronic Medical Record (EMR) is a record of what happened to a patient during their encounter(s) at a Care Delivery Organisation (CDO). It includes inpatient and outpatient environments, and is owned by the CDO. EMRs are used and maintained by healthcare practitioners to document, monitor, and manage health care delivery within a CDO (Garets & Davis, 2006; Zhang & Liu, 2010).

An Electronic Health Record (EHR) is a subset of health information from various CDOs where a patient has received care. EHRs are managed by a central government body in regions where such a body exists, and they provide a means of communication among clinicians contributing to a patient's care. EHRs are considered to be more trustworthy than PHRs since they contain information entered by medical care practitioners unlike PHRs (Garets & Davis, 2006; SITA, 2010; Zhang & Liu, 2010).

A Personal Health Record (PHR) is a complete and accurate summary of an individual's health and medical history, and conforms to any available nationally recognised interoperability standards. PHRs are initiated and maintained by an individual and include data from an individual's EMRs and EHRs, among other sources (Ed-informatics.org, 2012; Zhang & Liu, 2010).

Caligtan & Dykes, (2011) highlight the data components of EMRs, EHRs and PHRs as depicted in Table 2-2 below. The table lists the different functionality found in EMRs, EHRs and PHRs and highlights the distinct features and functions found in PHRs, which are:

- (i) Individual ownership of the health record.
- (ii) Inclusion of family history and allergy list.

The items highlighted in Table 2-2 are directly related to the key features of PHRs.

Table 2-2: Comparison of EMR, EHR and PHR functionality , adapted from (Caligtan & Dykes, 2011)

Comparison of Functionality		
EMRs	EHRs	PHRs
<ul style="list-style-type: none"> • Computerised order entry • Results retrieval • Scheduling and registration • Electronic messaging with other care providers within the group • Note documentation • Electronic prescribing • Disease management protocols • Clinical coding for billing purposes 	<ul style="list-style-type: none"> • Patient Demographics • Progress notes • Problem lists • Medications • Vital signs • Past medical history • Immunisation records • Laboratory data • Radiology reports • Electronic prescribing • Disease management protocols • Clinical coding for billing purposes • Consumers can access portions of the EHRs via patient portals 	<ul style="list-style-type: none"> • Patient demographics • <i>Family history</i> • <i>Allergies</i> • Medications • Past medical/surgical history • Past medical history • Immunisations records • Laboratory data • Radiology reports • <i>Consumers decide how much to contribute and have ownership of maintaining their records</i>

Although EMRs, EHRs and PHRs share a common set of functionality, PHRs focus on empowering individuals to be directly involved in the management of their health information. A PHR should include as much relevant data as possible over an individual's lifetime, from multiple sources, including various health care facilities as well as allowing personal data input by the individual (Tang, Ash, Bates, Overhage, & Sands, 2006).

This section has introduced and discussed eHealth and the classification of health information by EMRs, EHRs and PHRs. This research focuses on PHRs. A detailed discussion of PHRs is presented in section 2.5. Electronic Health Information faces a number of privacy concerns which

may hinder its wide spread adoption. The next section discusses privacy concerns associated with eHealth information and security mechanisms that can safeguard against them.

2.3 Privacy Concerns and Security Mechanisms

It is natural that patients may want their health information to be kept private and only accessed by medical care providers or individuals whom they have given permission. The terms privacy and security are often used when discussing health information. These two terms are related but have different meanings, hence it is important to clearly define them. For the purposes of this research, security is defined as a strategy whose outcome is privacy. For example, let us consider a doctor who desires to courier medical test results to one of his or her patients. The doctor seals the test results in an envelope before passing them on to a courier service. In this case, the security mechanism used is the envelope and the goal is to ensure that the privacy of the patient is not violated. The courier service will require the recipient (patient) to identify themselves before they are given the test results. The identification process (authentication) ensures that the results are delivered to the right person hence privacy is not compromised. However, if the patient is unable to receive his or her test results, a trusted third party may be authorised to receive them instead. The patient can grant authorisation by signing a letter to that effect. The person collecting the test results can then show the letter to the courier service delivery person. Security must be implemented to ensure privacy but security alone does not guarantee privacy. For example, the courier personnel may open the envelope, access the information and then reseal it. The behaviour amongst all participating agencies affect privacy (Herold, 2002). Health information privacy is an individual's right to control the acquisition, use, or disclosure of their identifiable health data. It is essential for any technology that collects and uses personal data (Avancha, Baxi, & Kotz, 2012).

The low adoption of PHRs and related technologies may be attributed to concerns that individuals have as regards to the safety of their records and the lack of enabling systems (Masiza, Mostert-Phipps, & Pottas, 2013). This is in contrast to EMRs whereby individuals trust healthcare organisations to protect personal information from wilful or accidental disclosures (Angst & Agarwal, 2009; US DoH, 2006). Mechanisms should be put in place by eHealth software developers to ensure that the privacy of health information is not entirely dependent on trust.

The remainder of this section focuses on identifying the threats to health information privacy, and the security objectives of this research in relation to the confidentiality, integrity and accessibility (CIA) model. The section will conclude with a review of existing security mechanisms that can be used to address the privacy needs of this research in relation to the CIA model.

Rindfleisch, (1997) identifies the following privacy threats to electronic health information:

- (i) Accidental disclosure by healthcare personnel. For example, an email message may be sent to an incorrect address.
- (ii) Data breach by an insider: insiders who access patient information and transmit it to outsiders for profit or for some other purpose of malice.
- (iii) Data breach by an outsider: an outsider who enters a physical facility and gains access to the system.

These threats are summarised in the form of security goals of this research:

- (i) An individual should be able to decide who can access their information and under what conditions. In case the information is accidentally sent to a wrong person, the recipient should not be able to access it.
- (ii) Storage providers should not be able to interpret an individual's stored information
- (iii) If information is leaked through a non-targeted exploit the medical information and patient identities should not be associated. All the personally identifiable information should remain unreadable.

The goals identified are discussed below in relation to the Confidentiality, Integrity and Availability model (CIA).

2.3.1 CIA Triad Model

The main objective of information security is to provide a trusted and protected environment for information assets and preventing and minimising the impact of security incidents. Information security is described as the sum of three core requirements namely: confidentiality, integrity, and availability. These are the three requirements that users demand from information systems, and are the cornerstones of any well-designed information security program. Together, confidentiality, integrity and availability are known as the “CIA triad,” and are illustrated in Figure 2-1. (Solomon & Chapple, 2005). The discussion of PHR security is guided by the CIA TRIAD model.

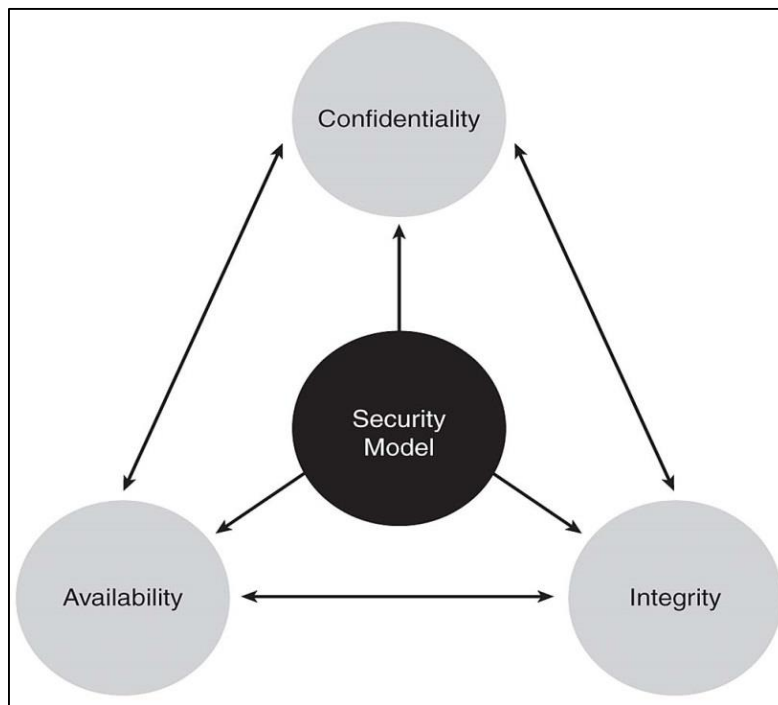


Figure 2-1: CIA Triad Model, adapted from (Solomon & Chapple, 2005)

Confidentiality

Confidentiality is concerned with ensuring that information can only be accessed by personnel who have been authorised to do so. For example, an individual may not be comfortable with sharing his medical records with his or her employer, but may be comfortable with sharing the same information with his or her spouse. Medical information is therefore deemed to be confidential. Confidentiality is one of the privacy goals of this research. Some of the measures used to ensure the confidentiality of electronic information are discussed in Section 2.3.3.

Integrity

The basic definition of integrity is ensuring that data may be modified only through an authorised mechanism. Integrity involves protecting data from the following types of unauthorised modification:

- (i) Unauthorised users altering data (such as a cracker breaking into a database and altering records).
- (ii) Data being altered through an inappropriate mechanism (such as a power surge causing database corruption).

Compromised medical data can put an individual's life at risk. For example, if doctors obtain false medical information about an individual, they may recommend treatment that can put the individual's life at risk.

Availability

The third goal of information security programs is to guarantee the availability of information. Authorised users should access the data whenever the need arises. After all, an individual's health data is not useful if it is not available for its intended use.

The next section provides a detailed discussion of key concepts in information security and how they can be applied in relation to the CIA model.

2.3.2 Overview of information security concepts

The objective of this review is to define the key concepts concerned within information security in order to ensure proper contextual use in the literature review. The definitions of the concepts are derived from Zimmermann (1991).

Encryption is a method of disguising content, called plaintext, in such a way so as to hide its substance. Encryption results in un-interpretable content, called ciphertext. The process of reverting the ciphertext to the original plaintext is known as decryption. For example, health records can be encrypted before being stored on remote storage devices, and can later be decrypted on client devices. This process is known as cryptography. The cryptographic functions are mathematical functions which utilise a key (word, number or phrase) to encrypt the plaintext. It

should be noted that the same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on:

- (i) The cryptographic algorithm; and
- (ii) The secrecy of the decryption key.

A cryptographic algorithm plus all possible keys and all the protocols that make it work are known as a Cryptosystem. Pretty Good Privacy (PGP) is an example of such a system.

Two types of encryption exist namely:

Symmetric cryptography: One key is used for both encryption and decryption purposes. Everyone involved in the communication has to have the private key.

Public-key cryptography: Public-key cryptography is an asymmetric scheme that uses a pair of keys. A public key for encrypting the data and an associated private key for decryption. The public key is published to the world, but the private key is kept secret. Anyone wishing to communicate with an individual can do so by encrypting content using the recipients public key. Only the recipient's private key can be used to decrypt the message. It is computationally infeasible to deduce the private key from the public key.

2.3.3 Applying the CIA Model to Personal Health Records

This section classifies and discusses the security mechanisms in terms of the CIA model and how they can be applied to ensure the privacy of PHRs.

2.3.3.1 Confidentiality

Authorisation can be defined as the act of permitting an individual or computer program to access a predetermined data set. Authorisation helps in ensuring confidentiality since outside unknown parties cannot access the information deemed to be confidential. Access control mechanisms are the methods used to manage the authorisation process. Below is a discussion of the commonly used access control mechanisms.

- (i) **User Authentication:** Authentication ascertains the identity of an individual or document. User authentication is the way in which users prove their authenticity to confidential information. Usernames with their associated passwords are the most common user

authentication mechanism. This research makes use of user authentication before permitting users to access their medical records.

- (ii) **Discretionary Access Control:** Discretionary Access Control is a means of restricting access to users based on their identity. The controls are discretionary in the sense that a user given access to a resource is capable of sharing that capability with another subject. The identity of the users is the key to discretionary access control (Alhaqbani & Fidge, 2008). A Discretionary Access Control model could create privacy problems since a user who has been given access to health data is capable of sharing their access credentials with third parties. Discretionary Access Control helps address the issue of health information sharing. However, it necessitates some level of trust between the different parties. This research aims to use mechanisms that require minimal trust between the parties. However, unauthorised disclosure remains a problem.
- (iii) **Role Based Access Control:** Role-Based Access Control decisions are based on the roles that individual users have as part of an organisation. Users take on assigned roles (e.g. doctor, nurse or receptionist in our case). Access rights (or permissions) are then grouped by role name, and the use of resources is restricted to authorised individuals. User membership in roles can be revoked as needed (Alhaqbani & Fidge, 2008). A role-based access control system may be suitable for use in PHRs. An individual is the primary administrator of their records and they authorise their doctors and related personnel to access their health records.

This section has discussed three access control mechanisms namely: User authentication, Discretionary Access Control and Role Based Access Control. User authentication is the most basic of the three and should be implemented by PHR applications. Discretionary Access Control was found not to be suitable for use in PHR applications because it requires a high level of trust, Role-based access enables an individual to share the health information as needed. For example, a dentist may not need access to an individual's full medical record. The next section reviews various security measures that have been used by other researchers addressing the same problem.

Measures to ensure security of records

Fernández-Alemán *et al.*, (2013) carried out a systematic literature review of security and privacy in EHRs. They found 23 articles that used symmetric key and/or asymmetric key schemes and 13 articles that employed the pseudo anonymity technique amongst other techniques. This discussion focuses on how private and public key cryptography is being utilised in the electronic health field. The articles reviewed were selected from the Fernández-Alemán *et al.*, (2013) literature study because they closely mirror the security goals of this study.

Patient Controlled Encryption (PCE)

Benaloh *et al.* (2009) propose a design named “patient controlled encryption (PCE)” that allows patients to selectively share records as desired. Their system partitions the patient’s record into a hierarchical structure as depicted in Figure 2-2, each portion of which is encrypted with a unique key.

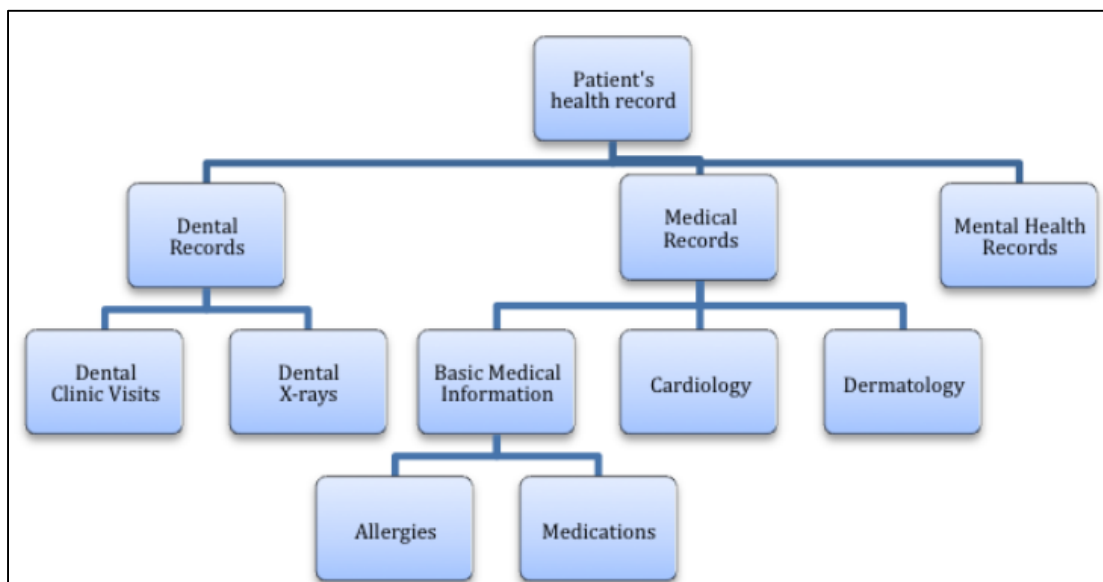


Figure 2-2: Hierarchical structure of medical records (Benaloh *et al.*, 2009)

The patient is required to store a root secret key from which a tree of sub keys is derived. The patient can selectively distribute the sub keys for decryption of various portions of the record. This implies that a sub key given to a dentist will differ from one given to a pharmacist. The PCE presents a way for securing patient health information on a storage medium. However, the system burdens the patient with key management tasks. The patients must manage root keys and all the

associated sub keys in case of symmetric key PCE. One flaw of the system is that a patient cannot revoke access for individuals. When a key is revoked, all associated users lose access.

Ciphertext policy Attribute based Encryption (CP-ABE)

CP-ABE is a type of identity-based encryption with the following properties

- (i) One public key.
- (ii) Master Private Key used to make more restricted private keys.
- (iii) Very expressive rules for which private keys can decrypt specific ciphertext.
- (iv) Private keys may be labelled with attributes.
- (v) CipherTexts have decryption policies. The policies specify who can decrypt the ciphertext (Bethencourt, Sahai, & Waters, 2007).

CP-ABE consists of a master key, a public key, a set of attributes, a set of private keys, and four fundamental algorithms (Setup, Encrypt, Key Generation, and Decrypt) in addition to one optional algorithm (Delegate).

Setup: takes an implicit security parameter to generate both the Master Key (MK), which is kept hidden from all users, and the Public Key (PK), which is shared with all users.

Key Generation (MK, S): generates a user private key (SK) using the master key MK and a set of attributes S that describes the owner of the key.

Encrypt (PK, M, A): generates ciphertext (CT) for the message M using the public key PK and associates it with an access policy A. The intent is that only users with keys that satisfy A can decrypt the ciphertext CT.

Decrypt (PK, CT, SK): decrypts the ciphertext CT in association with the public key PK and the user's private key SK and generates the original message M if and only if the set of attributes S that is associated with the private key SK satisfies the access policy A that was associated with the ciphertext CT.

Delegate (SK, S'): generates a private sub-key SK' from the private key SK, and associates it with a sub-set S' of the user's attributes S.

Key Management

There are three types of keys in CP-ABE (master key, public key, and private key):

- (i) **Master Private Key:** A private key that is used to generate users' private keys. This key is not shared with any user, provider, or third party.
- (ii) **Public Key:** A public key that is needed to encrypt or decrypt data in CP-ABE systems. This key is shared with all users, providers, and systems that need to authenticate the PHR.
- (iii) **Private Key:** A unique key that will be generated for each entity when it joins the system. This key uniquely describes each entity with the associated attributes. The users will use their keys to gain access to data that was authorised for them. This key should be accessible only by its owner.

The CP-ABE scheme has a slightly high computational cost for patients due to re-encryption of records when updating access policies. If the master key is stored on a hard disk, the CP-ABE scheme becomes vulnerable to crackers. A similar approach (Attribute Based Encryption) is employed by Narayan *et al.*, (2010) in their model of securing health records in a cloud environment. Unlike the CP-ABE, their approach assumes that there is a trusted authority who generates keys for users of the system.

This section started off by defining key concepts in cryptography with the aim of reviewing security measures that are being used to secure health records. The concept of patient controlled privacy using either asymmetric or symmetric cryptography as presented by Benaloh *et al.*, (2009), was reviewed and it was noted that the concept is theoretically possible. However, the patients will be burdened by key management tasks, which may affect the overall usability of a system designed from their model. The CP-ABE scheme eases the key management task hence this research will use this approach.

2.3.3.2 Ensuring Integrity using Digital Signatures

Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. The basic manner in which digital signatures are created is as follows:

- (i) A message hash is generated from the contents of information to be sent. The message hash is encrypted with a sender's private key to generate the digital signature.
- (ii) The digital signature is then sent with the information to a recipient.
- (iii) The recipient calculates the message hash of the received message (value one)
- (iv) The recipient also extracts the message hash received with the message (value two), by using the sender's public key and their digital signature.
- (v) If both values one and values two are equal, then the message has not been tampered with.

Digital signatures can be used to ensure that a medical record has not been altered by any unauthorised person. Unauthorised alterations may put an individual's health at risk. If medical personnel is presented with incorrect medical history, they may prescribe medication which may harm the patient.

2.3.3.3 Ensuring Availability

Measures should be put in place to ensure the un-interrupted flow of information either in offline/online mode.

This section has highlighted the differences between security and privacy. CIA model was introduced and guided the review of the different concepts related to health information security. The review of the work done by other researchers in relation to the security and privacy of health records highlighted various measures and techniques which are currently being used and can be adapted to meet the needs of this research. It is important to choose mechanisms that least affect the usability of the application and are sensitive to the limited computational resources available on mobile devices.

2.4 Legislation and guidelines

Section 2.3 discussed privacy threats and technical mechanisms intended to protect the confidentiality of eHealth records. Legislation and guidelines can also be used to protect eHealth records in given geographical regions. Section 2.4.1 discusses US guidelines while Section 2.4.2 focuses on South Africa.

2.4.1 US Guidelines

The Health Insurance Portability and Accountability Act (HIPAA) enacted by the United States Congress in 1996, is the Federal Law that applies to the U.S. healthcare industry. HIPAA provides conceptual guidelines that must be strictly observed by organisations concerned with healthcare provision. HIPAA indicates that patients' privacy should be emphasised, and this principle can be applied to the health industry throughout the world (Ihs.gov, 1996; Kaelber & Jha, 2008; OCR Hipaa, 2003). A summary of the HIPAA privacy and security technical safeguards are described in Appendix B.

While the HIPAA Act of 1996 outlines the legal protections for PHR privacy and security, it only applies to “covered entities”, which include health plans, healthcare clearing houses and health care providers in the US. It is therefore used for reference purposes in this research study. A discussion of the legal guidelines and requirements applicable to South Africa is presented in the next section.

2.4.2 South African Legislation

The South African National Department of Health in their eHealth strategy (2012-2016) highlight the regulations affecting eHealth as (NDoH, 2012):

- (i) The Minimum Information Interoperability Standards (MIOS).
- (ii) Promotion of Access to Information Act, Act 2 of 2000.
- (iii) The Minimum Information Security Standard.

These regulations do not provide conformance guidelines for eHealth; rather they highlight how sensitive health information should be handled by government bodies and the private sector. The

Health Professions Council of South Africa (HPCSA) provides a set of guidelines for how health records should be accessed and shared in South Africa (HPCSA, 2008). These guidelines are:

- (i) Records should be complete and accurate.
- (ii) Records should be consistent.
- (iii) A standardised format should be used (for example, notes should contain in order the history, physical findings, investigations, diagnosis, treatment and outcome).
- (iv) Copies of the records should only be released after receiving proper authorisation from the data owner.
- (v) Attached medical documents such as diagrams and laboratory results should be clearly labelled.

The South African Department of Health released the National Health Normative Standards Framework for Interoperability in eHealth in South Africa (HNSF). One of the recommendations of the HNSF is that South Africa should adopt and adapt international eHealth standards such as HL7 CDA and CCD (NDoH & CSIR, 2014). This research presents a hybrid PHR management model in Chapter 4, which is informed by such international standards. The HNSF was released too late for consideration in the design of the Hybrid model. However, a reflection on the Hybrid PHR model and the HNSF is presented in Chapter 6.

Rishel (2009) of Gartner Research argues that explicit consent from the consumer supersedes most of the jurisdictionally-specific requirements for limiting data exchange. This section has discussed both US and South African guidelines for eHealth. The HIPAA technical safeguards and the HPCSA guidelines discussed will form the legal requirements for this research. The rest of the chapter focuses on PHRs and how the legislation and security guidelines discussed can be applied to them.

2.5 Personal Health Records

A brief overview of the evolution of PHRs and their benefits is highlighted in Section 2.5.1. Section 2.5.2 discusses PHR data encoding standards and motivates the standard chosen for this research. The section concludes with a discussion of PHR functional requirements.

2.5.1 Overview and Benefits

Szolovits *et al.* (1994) highlights the shortcomings of centralised patient management systems that directly exclude patients from the management of their health records. They propose a personal health system referred to as “Guardian Angel” that collects medical data, checks and interprets it, and explains to the subject medically relevant facts and plans. This was envisioned to improve the quality of medical decision making, increase patient compliance, and minimise medical errors.

The Guardian Angel is an active process that:

- (i) Engages in data collection, sometimes by interacting with the subject and sometimes by automatic tracking and recording instruments.
- (ii) Monitors the progress of medical conditions and the effect of therapy with respect to expectations and checks for side effects.
- (iii) Interprets facts and medically-related plans and helps explain them to the individual.
- (iv) Interfaces to information systems used by care providers, insurers, and researchers to provide access to personal medical history information as authorised by the individual.
- (v) Implements patient reminding and alerting functions, including reminders of scheduled therapy, medications and appointments, integrating these with personal scheduling tools.

The above discussion illustrates that the concept of patient-centred health care and PHRs in particular has and is being considered by other researchers.

The following benefits can be realised with PHRs (HealthIT.gov, 2013; Tang *et al.*, 2006):

- (i) They provide a unified summary of an individuals’ health history.
- (ii) They encourage family health management, in which care givers, such as those caring for young children and elderly patients, manage their care.
- (iii) They are easy to understand and use.
- (iv) They provide access to healthcare data from anywhere in the world.
- (v) They facilitate continuous communication between patients and physicians.

The benefits of PHRs have been well documented. It is important to review existing PHR standards before actual design and implementation is carried out. Standards exist to ensure that a given

product or service meets acceptable criteria of a given community. They are usually documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure quality (ISO, 1947).

2.5.2 Data Encoding Standards

PHRs should be encoded using best practices to ensure interoperability of systems that access/utilise the data. At present, several Standards Development Organisations (SDOs) are working to create frameworks for representing and exchanging the contents of EHRs and PHRs. The prominent standards are the Continuity of Care Record (CCR) by the American Society for Testing and Material International and the Clinical Document Architecture (CDA) by Health Level Seven (HL7) (Ferranti, Musser, Kawamoto, & Hammond, 2006).

Continuity of Care Record (CCR)

The Continuity of Care Record (CCR) standard was created by the American Society for Testing and Materials to enable physicians to collect patient care information in a structured, human-readable and transferable format (Ferranti *et al.*, 2006). This standard was incorporated by Health Level Seven (HL7) into their Clinical Document Architecture (CDA), hence this research focuses on the CDA standard.

Clinical Document Architecture (CDA)

HL7 is an international organisation focused on developing standards to enable the interoperability of different medical information systems (HL7, 2013). HL7 created the CDA as the standard format for exchanging clinical documents. CDA documents are coded in either XML or JSON (Huang, Tseng, Chang, & Taipei, 2010).

The HL7 has several working groups each concerned with an aspect of eHealth. One of such groups is the Mobile Health Work Group (MHWG), which is tasked with the creation, promotion and the maintenance of Mobile Health (mHealth) related standards and frameworks (MHWG, 2013).

Below is a discussion of the Personal Health Record System (PHR-S) standard by the MHWG. The PHR-S functions enable an individual to manage their health-related information (Donald,

Ritter, Spears, & Dyke, 2008). Figure 2-3 highlights the functions in the PHR standard and the focus of this research.

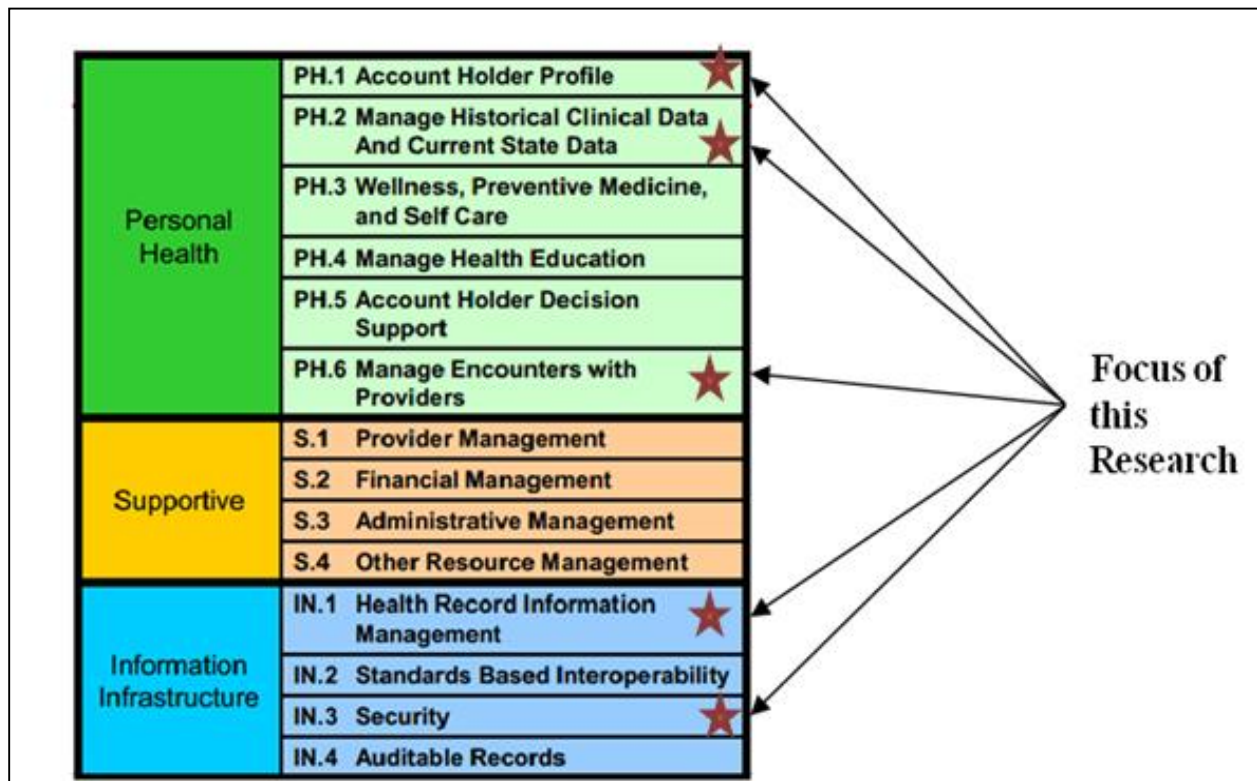


Figure 2-3: Standard Overview, adapted from (Donald T, 2010)

The functions (PH.1; PH.2; PH.6) were selected because they are closely related to the main objective of this research, that is, to facilitate the management of PHRs. The owner of the PHR is referred to as the Account Holder and he/she may be represented by the parent/guardian, or a designated representative (proxy) and one person can manage two or more accounts. This can be used as a basis for sharing PHRs with medical personnel, that is, an individual may permit a doctor to access their medical record. Historical health information as well as current health status should be captured and maintained in the PHR. One of the highlighted functions is PH.6. However, this research will exclude portions of PH.6 and will only focus only on the subset which is concerned with sharing of health data with medical providers. How the medical providers make use of the data is beyond the scope of this research. Appendix C has a detailed description of the function and sub-functions.

Information Infrastructure functions ensure that a PHR system provides information privacy and security (EHR Work Group, 2008). The functions (IN.1; IN.3) were chosen because they directly affect the management of PHRs and help in achieving research objective 3. Objective 3 is concerned with the design of the PHR management model and the implementation of the prototype applications. Health Record Information Management (IN.1) is concerned with the capturing, storage and reporting of the PHR systems, while IN.3 (Security) helps in ensuring the secure access to PHR system and PHR information by managing the sets of access control permissions granted within a PHR system.

The standards model will be used in the implementation of the model for PHRs. The Personal Health functions (PH.1; PH.2; PH.6) and Information Infrastructure Functions (IN.1; IN.3) represent the focus of this research, which is empowering individuals to manage their PHRs. The role of medical personnel is limited to accessing the data when authorised by their patients.

2.5.3 PHR Use Cases

A PHR can give patients peace of mind, since medical conditions such as allergies and current drugs are kept in one secure place and are easily accessible when needed (Blue Cross, 2013). WEDI, (2007), a workgroup for Electronic Data Interchange based in Virginia USA classifies PHRs as either tethered or untethered as defined below:

Tethered PHR: A PHR dataset that is linked to a provider, health plan, pharmacy or payer controlled data sets.

Untethered PHR: The dataset used to populate the PHR is completely standalone and the individual or care giver is the main source of health data.

This research and the discussion about use case scenarios focuses on untethered PHRs. US.DoH, (2007) provides a detailed use case of PHR data classified as:

Prototype Use case: describes the flows of the use case at a high level and facilitates initial discussion with stakeholders.

Detailed Use Case: documents all of the events and actions within the use case at a detailed level.

This discussion is focused on two use cases that is, the sharing of information between consumers (close family) and providers (health care professionals). The process of information sharing may be explained with the help of Figure 2-4. The figure shows interaction between a single target system and single requesting system.

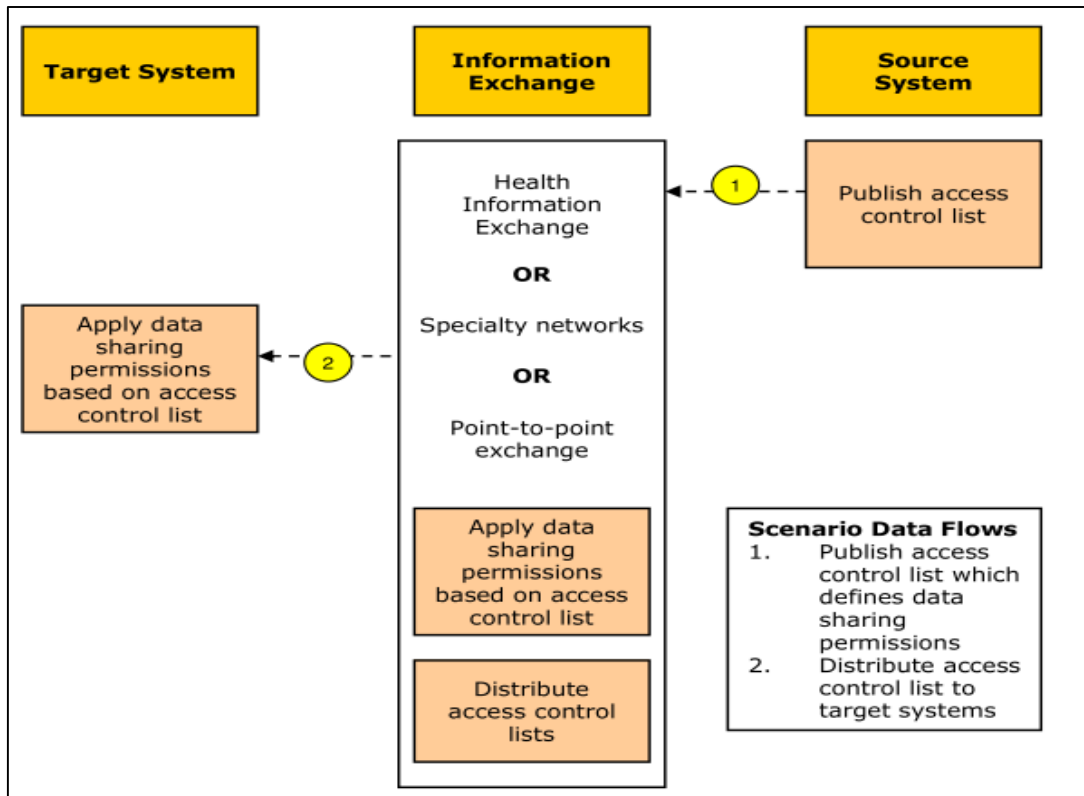


Figure 2-4: Create and Maintain Access Control Lists, adapted from (US.DoH, 2007)

The information flow illustrated inspired the design of the permissions algorithm used in the Hybrid PHR Management Model (Chapter 4). The next section discusses the requirements for PHR systems derived from the reviewed literature.

2.6 Personal Health Records Requirements

This section presents the requirements for PHR systems; they are categorised as functional, data and security and are discussed in Sections 2.6.1, 2.6.2 and 2.6.3 respectively.

2.6.1 Functional Requirements

The functional requirements were derived from the PHR standard by HL7; a subset of the functions is presented below and is grouped into two categories, namely:

- (i) Personal health functions: directly relate to health information management.
- (ii) Information Infrastructure functions: support the management of personal health information.

A detailed description of the functions is presented in Appendix B (Donald et al., 2008; EHR Work Group, 2008).

2.6.2 Data Requirements

The American Health Information Management Association (AHIMA) is dedicated to the effective management of personal health information needed to deliver quality health care to the public. The AHIMA has put together a set of procedures and forms individuals can use to construct their own personal health records (AHIMA, 2013). Below is a listing of the data that the AHIMA suggest should be contained in a PHR. Caligtan & Dykes, (2011) also present similar data requirements for PHRs. Hence, these are the data requirements for this research.

Table 2-3: PHR Data requirements, adapted from (AHIMA, 2013)

PHR Data
<ul style="list-style-type: none"> • Personal identification, including name and birth date • People to contact in case of emergency • Names, addresses, and phone numbers of your physician, dentist, and specialists • Health insurance information • Living wills, advance directives, or medical power of attorney • Organ donor authorisation • A list and dates of significant illnesses and surgical procedures • Current medications and dosages • Immunisations and their dates • Allergies or sensitivities to drugs or materials, such as latex • Important events, dates, and hereditary conditions in your family history • Results from recent physical examinations • Opinions of specialists • Important tests' results; eye and dental records • Correspondence between you and your medical provider(s) • Current health related educational materials • Any information you want to include about your health – such as your exercise regimen, any herbal medications you take and any counselling you may receive • Dietary practices, such as whether you are vegetarian, or on a temporary diet; especially if changes in your diet have produced changes in your health in the past.

A sample PHR record from Microsoft Health Vault (MHV) is presented in Figure 2-5 with the aim of highlighting the categories that can be contained in such a record, e.g. conditions, measurements, files, medications, health history, personal profile and fitness. It should be noted that the Continuity of Care Document (CCD) and the Continuity of Care Record (CCR), which are discussed in section 2.5.2 are listed as suitable of the files formats in MHV.

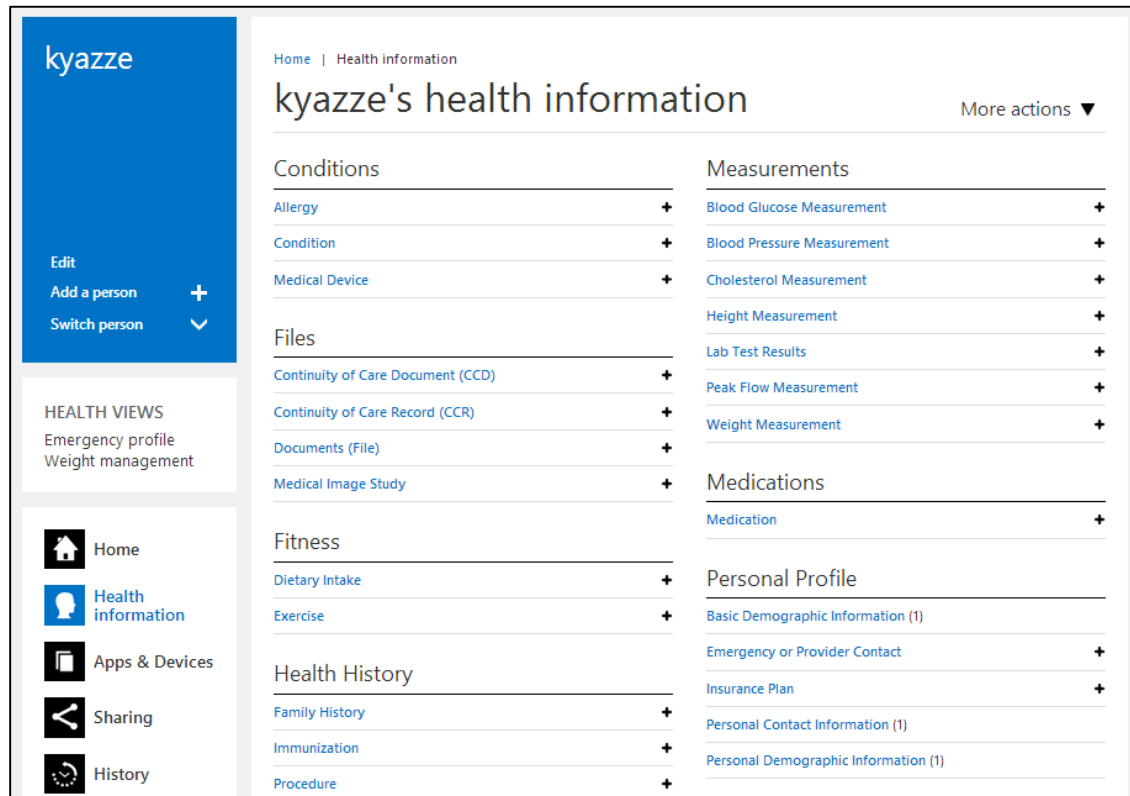


Figure 2-5: A sample PHR by Microsoft Health Vault, adapted from (MSHV, 2013)

This research focuses on PHRs and how they can be managed ubiquitously using mobile devices. The key difference between an EHR and a PHR is the management and access control. Whereas a patient may not have access to their EHR, they do have full access to their PHR. A PHR account holder can manage multiple PHRs, for example a mother can manage the accounts of her children while an EHR account holder can only manage a subset of his or her own personal data. The intended users of PHRs are individuals who are interested in taking an active role in the management of their health records.

2.6.3 Security and Privacy Guidelines

This research abides by the HIPAA technical guidelines and the HPSCA guidelines discussed in section 2.4. The research also utilises the privacy notice by HealthIT.gov, (2013), which is illustrated in Figure 2-6. The privacy notice was designed to be a standardised template that can be used by PHR companies to inform customers about their privacy and security policies. The PHR model privacy notice does not specify whether medical health data is anonymised.

Release				
Do we release your PHR Data for these purposes?	[Yes/No]	We release...	Personal Data	Statistical Data
		For marketing and advertising	[Yes/No]	[Yes/No]
		For medical and pharmaceutical research	[Yes/No]	[Yes/No]
		For reporting about our company and our customer activity	[Yes/No]	[Yes/No]
		For your insurer and employer	[Yes/No]	[Yes/No]
		For developing software applications	[Yes/No]	[Yes/No]
Do we require Limiting Agreements that restrict what third parties can do with your Personal Data ?	[Yes/No]			
Do we stop releasing your Personal Data if you close or transfer your PHR ?	[Yes/No]			
Secure				
We have security measures that are reasonable and appropriate to protect personal information , such as PHR Data , in any form, from unauthorized access, disclosure, or use.				
Do we store PHR Data in the U.S. only ?	[Yes/No]			
Do we keep PHR Data activity logs for your review?	[Yes/No]			

Figure 2-6: PHR model privacy notice (HealthIT.gov, 2008)

2.7 Conclusion

The objective of this chapter was to address part of Research Question 1, which concerns the requirements for ubiquitous management of PHRs in South Africa. A review of eHealth terminology identified three classifications of eHealth information. These are EMRs, EHRs and PHRs, a clear understanding of the differences between the terms helped in the identification of PHR requirements. PHR data encoding standards were reviewed and the Clinical Document Architecture (CDA) by HL7 was found to be the most applicable to South Africa. HL7 provides a PHR standard, which can be adapted for this research. Mechanisms that can be used to ensure the privacy of eHealth information were discussed in relation to the CIA model. The CP-ABE scheme was chosen as the main mechanism for ensuring patient privacy. This is because an access policy is embedded within the ciphertext; hence patients can easily revoke the access of a given medical practice by removing that practice's attributes from the access policy. Anonymisation, which can be used to safeguard health records from un-authorized access, is another mechanism suitable for

this research. Chapter one identified the limited focus on PHR management in South Africa. This chapter has highlighted the importance of PHRs and how they can be used to improve personal health care, because PHRs are solely managed by individuals, which is an important aspect that differentiates them from EMRs and EHRs.

This chapter completes the first phase of DSRM by investigating the research problem and motivating its relevance. According to the guidelines by Hevner *et al.*, (2004), the requirements identified are seen as an artefact, which can be used by researchers to address a similar problem. The requirements were categorised as Functional: Section 2.6.1, Data: Section 2.6.2 and Security guidelines: Section 2.6.3

The next chapter will review existing Mobile health applications and PHR architectures with the aim of identifying a suitable architecture that can support ubiquitous management of PHRs in South Africa.

Chapter 3: Mobile Health Applications and Architectures

3.1 Introduction

The objective of this chapter is to review existing mobile health (mHealth) systems that could be used to support ubiquitous access and secure sharing of PHRs and their architectures. A classification of existing mHealth interventions is presented with the aim of highlighting the existing gaps in personal health information management and illustrating how this research fits into the bigger picture of mHealth. The criteria used in guiding the evaluation process of the selected set of PHR applications were determined from existing literature. The shortcomings of existing applications were identified with the aim of these being addressed in the proposed model. The existing PHR architectures are also discussed with the aim of selecting one for use in South Africa. The contribution of this chapter is the evaluation criteria and analysis of existing applications and architecture for PHRs in South Africa.

The introduction of information and communication technology (ICT) in the health sector has resulted in changes in clinical practices; some of these changes included the facilitation of medical services at a distance. The use of ICT in the health sector is defined as electronic health (Rašković, Milenković, & Groen, 2008). The recent developments in ubiquitous communication have the potential to provide individuals with tools that enable them to monitor aspects of their health on a 24 hour basis. The emerging concept is mobile health (mHealth), which can be defined as the provision of health-related services via mobile communications. Mobile health has emerged as an important sub-segment of the field of electronic health (Vital Wave Consulting, 2009). Mobile health represents the evolution of eHealth systems from desktop telemedicine platforms to mobile configurations. It complements eHealth by making health services available to individuals who may not have access to computers but have personal mobile devices. Mobile health can have a significant impact on the vision of eHealth in South Africa.

3.2 Mobile Devices in HealthCare

The explosion of mobile phone usage in South Africa has the potential to improve health service delivery on a massive scale. For example, mobile technology can support inclusive health systems by enabling health workers to provide real-time health information and diagnoses in rural and marginalised areas where health services are often scarce or absent altogether (NDoH, 2012). Mobile devices are currently being used worldwide in various health related activities ranging from home monitoring of elderly patients to being used as portable laboratory microscopes (Mukandatsama & Wesson, 2013; Sumriddetchkajorn, Somboonkaew & Chanhorm, 2012).

Although mHealth is a new area of scientific development, researchers have been laying the groundwork over the past four decades. Smart mobile devices provide sensing, analytic and presentation capabilities. These features can provide an unprecedented view of a person's health status and behaviour patterns (Kumar, Nilsen, Pavel, & Srivastava, 2013). Some of the benefits provided by mHealth are:

- (i) Real-time monitoring and detection of changes in health status.
- (ii) Supporting the adoption and maintenance of a healthy lifestyle.
- (iii) Providing rapid diagnosis of health conditions.
- (iv) Facilitating the implementation of interventions ranging from promoting patient self-care to providing remote healthcare services.

The literature about mHealth is vast; hence it is important that a classification of mHealth interventions is discussed in order to better understand the design space and how this research fits into the bigger picture of mHealth.

3.2.1 Classification of mHealth Applications

Mobile health has the potential to turn mobile devices into personal labs that continuously assess a person's physiology, behaviour, social context and environment exposure (Kumar *et al.*, 2013). In recent years, a number of researchers have begun to use mobile phones as platforms for delivering health interventions. A classification of the types of health interventions and applications that have been implemented is summarised in Figure 3-1. The figure illustrates the design space and highlights where this research falls in mHealth (Klasnja & Pratt, 2012; Vital Wave Consulting, 2009).

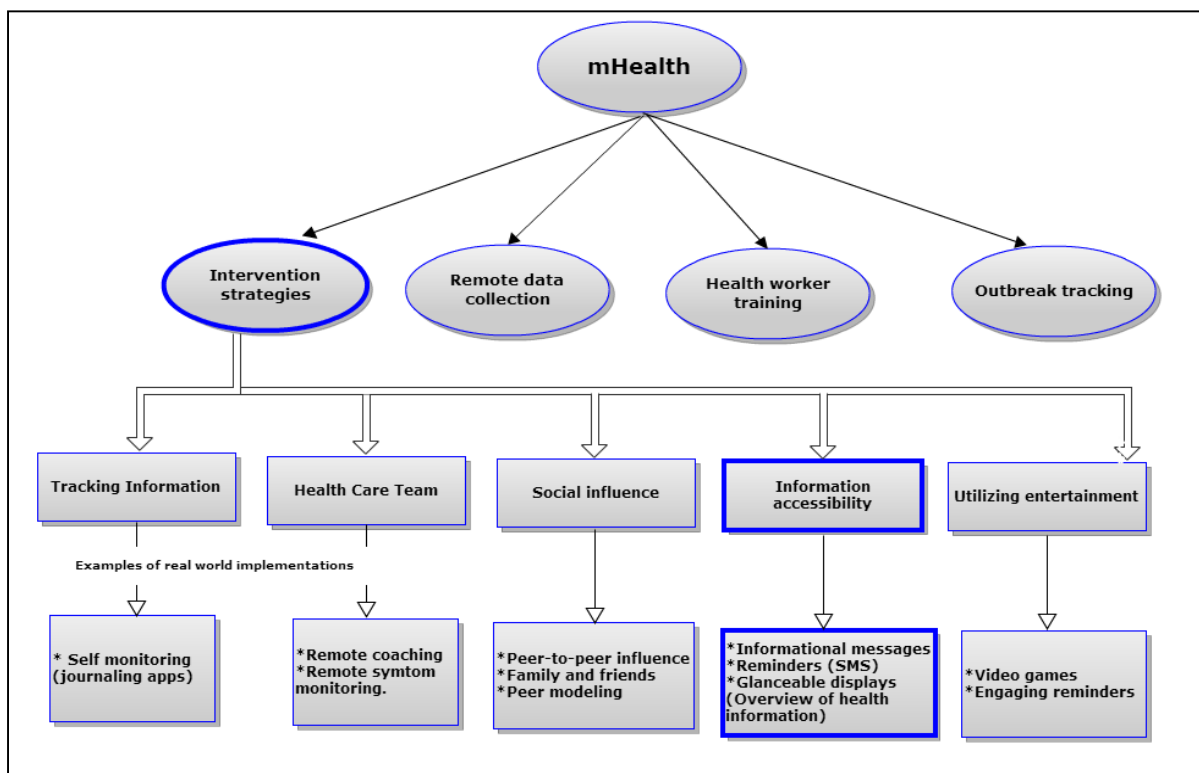


Figure 3-1: Illustration of mHealth design space, adapted from (Klasnja & Pratt, 2012)

Self-monitoring is a core strategy of many interventions in, which the phone is used to track health-related behaviours and parameters. For example *Myfitness pal* helps users to track their eating habits and body weight. It is claimed to offer nutrition facts for hundreds of foods (*Myfitnesspal.com*, 2013). A second strategy involves sharing the captured data with a healthcare team, keeping them informed about the patients' condition. For example, *Healthspek* allows individuals to share their medical information with various health providers. A detailed review of Healthspek is provided in Section 3.5.

A third strategy leverages the social influence of friends and support groups to influence desired behaviour. For example, *Lose It*, uses the influence of friends to help individuals achieve their weight goals (*Loseit.com, 2013*). A fourth strategy aims to increase the accessibility of health information. The fifth strategy utilises entertainment to engage individuals with their health goals. The discussion above helps to highlight that health information accessibility is one of the mHealth intervention strategies, which are currently being addressed by other researchers.

3.2.2 Motivation for personal health information management

Accessing patient medical records outside the hosting authority remains an obstacle that needs to be addressed (Mohamed, Tawfik, Al-Jumeily, & Norton, 2011). Patients have difficulty accessing their health data for personal health activities such as decision making and health planning (Steele & Min, 2010). For example, let us consider a fictional person named John. John's career places him in a different country every 5 years. His medical records are scattered across Uganda, South Africa and Namibia. Whilst Electronic Medical Records (EMRs) in a country like South Africa are helpful, John's physicians in South Africa will not have the complete details of his medical history. Figure 3-2 illustrates the above scenario.

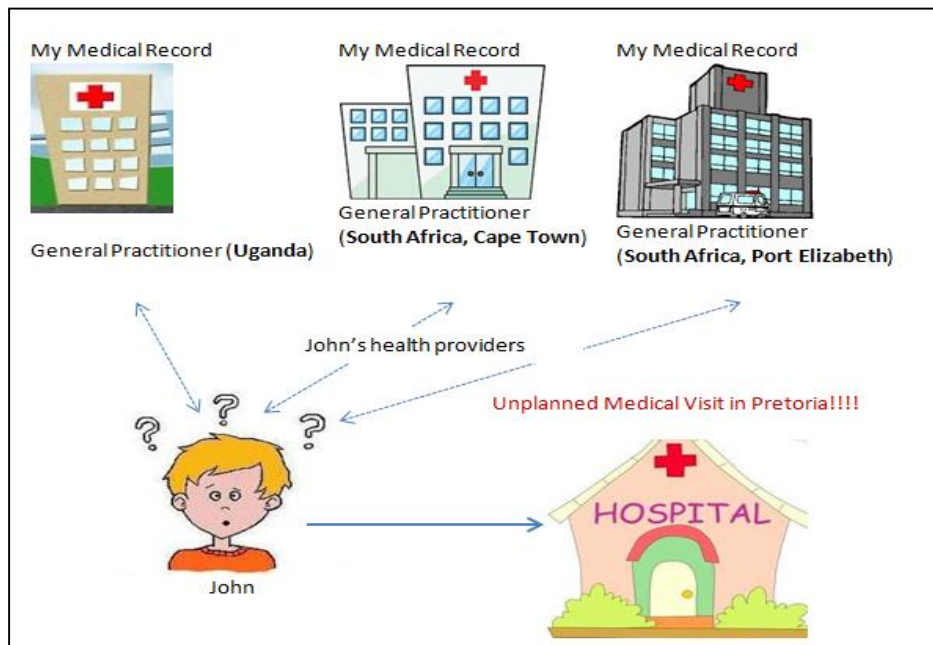


Figure 3-2: Necessity for personal health information management

Personal health information management, and usage of contextual information with health information could benefit from mobile-based solutions (Klasnja & Pratt, 2012). Among all the

barriers to the implementation of EHR systems, privacy and security concerns relating to patients' medical records are arguably the most dominant according to various literature studies. However, the lack of comprehensive EHR systems cannot be ignored (Sun & Fang, 2010). A number of researchers have tried to address the problem of ubiquitous access to health records; together with the security measures to guarantee the privacy of the records. Whilst the security barriers identified are related to EHRs, they affect PHRs in a similar way. Mechanisms that ensure the privacy of electronic health data were discussed in chapter 2. The next section discusses the different categories of PHRs and motivates the category chosen for this research.

3.3 PHR categories

A categorisation of PHRs is carried out to help focus this review on the relevant category, which is in line with this research. The International Organisation for Standardisation (ISO) has broadly divided PHRs into 4 general categories (ISO/TR20514, 2005):

- (i) A self-contained EHR maintained and controlled by the patient/consumer.
- (ii) A patient-controlled PHR maintained by a third party such as a web service provider.
- (iii) A component of an integrated care EHR maintained by a health provider and controlled at least partially by the patient/consumer.
- (iv) A component of an integrated care EHR maintained and controlled by the patient/consumer.

The health information category (i) is entirely patient managed. That is, individuals can make use of local storage media such as USB flash drives, paper files and compact disks. A limitation of this category is that: the devices can be misplaced, causing data loss and possibly leading to exposure of confidential health information. This limitation can be mitigated by category (ii). In category (iii), a web service provider provides storage, backup, secure access to PHRs. The categories of (iii) and (iv) would be the most ideal if hospitals located in different geographical locations (for example Uganda and South Africa) shared data about individuals. Unfortunately, such infrastructure is not in place. This leaves category (ii) as the most viable option for individuals residing in countries where comprehensive national EHR systems are not in place, for example South Africa.

3.4 PHR Evaluation Criteria

Well established evaluation criteria help to prevent reviewer bias when discussing existent systems. This review is going to be restricted to category (ii), which covers PHRs that are held by a third party web service provider on behalf of the users. Kharrazi *et al.*, (2012) carried out an evaluation of features and functionality of mobile PHRs. Nineteen standalone PHR applications were evaluated. The selected applications were limited to:

- (i) PHR applications that stored data on the phone's local storage.
- (ii) Disease specific applications, for example high blood pressure monitor were excluded from the review.
- (iii) PHR applications costing not more than \$100.

The PHRs that were selected were evaluated using the following PHR data elements as criteria: *Conditions, Procedures, Medications, Providers, Allergies, Labs, Immunisations, Family History, Emergency Contact and Insurance*. Kharrazi *et al.*, (2012) observed that the data elements and application features of current mobile PHRs are often incomplete and are not properly secured. For example, some of the reviewed applications did not have mechanisms in place to ensure the confidentiality of the medical data. They also observed that the main difference between free and paid versions of PHRs were: *import/export capabilities and support for multiple health records*. They recommend that future research and development of mobile PHRs should include all recommended data elements and the required application features, which they identified as: *data security and privacy, and import/export of data/images*. Ideally, phone features such as the camera can be integrated into PHRs to scan and import paper documents.

Whilst data elements are important in PHRs, their use as the sole criteria for evaluation purposes is limited since the ease of use, data validation, and related factors, are not evaluated.

Kim & Johnson, (2002) also evaluated 12 PHR applications using five functions and associated requirements as criteria. Table 3.1 summarises the criteria used.

Table 3-1: Criteria for PHR evaluation (Kim & Johnson, 2002)

#	Function	Requirements
1.	Providing everywhere access to PHRs	(i) Secure password-protected patient access information (ii) Capacity to provide authorised provider access (iii) Capacity to provide directed emergency access
2.	Providing medical summaries for health care providers	(i) Accurate entry of medical conditions and medications (ii) Verification of laboratory test results (iii) Verification of diagnostic study results (iv) Verification of immunisations, including information about dates and sequences
3.	Portal to patient-specific consumer-level health care information	(i) Capacity to provide links to consumer health care information
4.	Providing interpretive information about laboratory test and diagnostic results	(i) Capacity to interpret laboratory test and diagnostic results
5.	Serving as a database of information for patient-specific self-monitoring and disease management	(i) Verification of monitoring study results (ii) Capacity to interpret monitoring study results (iii) Capacity to provide evaluation and treatment recommendations (iv) Capacity to provide secure communication between patients and providers

The set of functions used by Kim & Johnson (2002) as evaluation criteria for PHRs are similar to the PHR functions identified in Section 2.6.1. These functions will be used as the main evaluation criteria. They will be complemented by the data elements used by Kharrazi *et al.*, (2012).

3.5 Review of Existing Applications

Avancha *et al.*, (2012) refer to Microsoft Health vault (MHV) and Google health (GH) as two well-known PHR services. However, since Google health was permanently discontinued because of the lack of widespread adoption (Google, 2013), MHV is reviewed to gain an understanding of what constitutes a typical PHR system. A selected set of mobile phone applications were also reviewed. The applications were selected from the European Directory of Health Apps 2012-2013, which contains key information on health-oriented applications that are recommended by patient groups and empowered consumers. These applications are grouped by specialisation (EPDA, 2013). This review was limited to two specialisations, namely: Medical Records and Doctor patient communication.

3.5.1 Microsoft Health Vault (MHV)

Figure 3-3 contains an illustration of MHV.

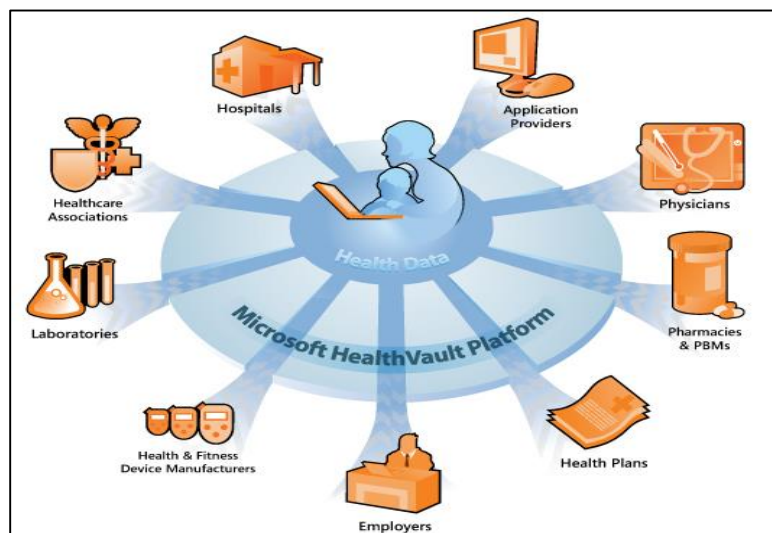


Figure 3-3: Microsoft health vault Platform Overview (Microsoft, 2013)

MHV is a cloud-based platform that offers a privacy and security-enhanced foundation on which a broad ecosystem of solution providers, device manufacturers, and developers can build innovative new health and wellness management solutions (Microsoft, 2013). An account holder can manage their conditions, measurements, files, medications, fitness, health history and personal profile information. Sharing can be enabled by giving limited or full access to select individuals. An API is provided for third party apps that enhance the functionality of MHV. The categories of

the health information adhere to the PHR standard discussed in Chapter 2. MHV provides Software Development Kits (SDKs) for specific mobile platforms, which include Android, Windows and iOS.

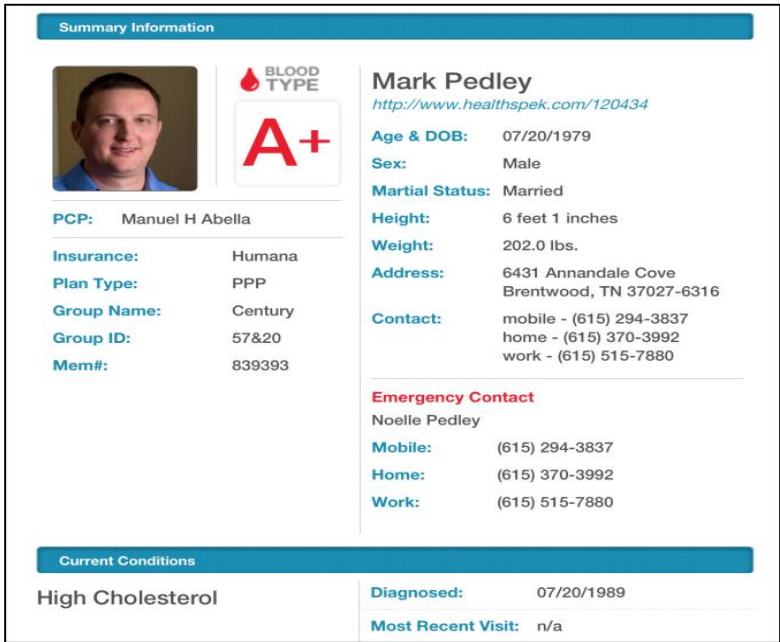
MHV is a web-based platform hence offline data storage capabilities are not supported. However, the offline capabilities can be built into third party applications that make use of the platform. Whilst MHV meets most of the PHR requirements, it does not satisfy the needs of a mobile user since it is primarily accessed through a web interface.

3.5.2 HealthSpek

This application was chosen as the winner of the AppyAwards 2013 under the medical category. The Appy awards are dedicated to acknowledging creativity and excellence in application design (Appy Awards, 2013). Healthspek enables individuals to keep track of their medical history and allows continuous updates with health providers (HealthSpek, 2013).

Key functionality includes:

- (i) myDashboard, which is a customisable home page with “Speks” to help each family member manage their health and wellness; such as “Med Refills,” “Health Tips,”
- (ii) MyProfile allows the user to record doctors, insurance, emergency contacts, a personal picture and a signature.
- (iii) MyRecords is the medical chart of Healthspek. Sections include conditions, medications, labs, vitals, imaging, allergies, history, and more




Summary Information	
	BLOOD TYPE A+
Mark Pedley http://www.healthspek.com/120434	
Age & DOB:	07/20/1979
Sex:	Male
Marital Status:	Married
Height:	6 feet 1 inches
Weight:	202.0 lbs.
Address:	6431 Annandale Cove Brentwood, TN 37027-6316
Contact:	mobile - (615) 294-3837 home - (615) 370-3992 work - (615) 515-7880
Emergency Contact Noelle Pedley	
Mobile:	(615) 294-3837
Home:	(615) 370-3992
Work:	(615) 515-7880
Current Conditions	
High Cholesterol	Diagnosed: 07/20/1989
	Most Recent Visit: n/a

Figure 3-4: Sample HealthSpek Patient Profile (HealthSpek, 2013)

HealthSpek can be categorised as a free standing PHR application where the patient is tasked with the management of their health records. Patients can authorise doctors to access their health records through a web site. The patients pass on unique codes, which doctors can use to gain access; these codes can easily be changed by an individual using the mobile application.




ChartNow
Your Patient's Health Record

Enter the code provided by your patient:

Chartnow requests that you make the [calculation] below before submitting your login information:

2 + 8 = ?

Submit

Figure 3-5: Doctor access website (HealthSpek, 2013)

We are interested in the actual design of the PHR management model and its security mechanisms, which cannot be obtained from HealthSpek. The HealthSpek Application provided design inspiration for the mobile application prototype that was implemented as part of this research (Section 4.5).

3.5.3 Capzule PHR

Capzule PHR is a password-protected PHR application. It empowers patients to manage appointments with their doctors, manage medications and easily share summaries of their health information. Whilst the application facilitates ubiquitous access to health records, this functionality is offered with a range of other features, which may not be desired by certain individuals who are mainly interested in PHR management. This research is limited to the management of PHRs, which is not the case with Capzule PHR.

Summary	
Summary	
Name	Descartes Gregory
Age & DOB	41 yrs 12/19/1971
Gender	Male
Marital Status	Married
Blood Type	A+
Height & Weight	0cm 0kg BMI 0.0
Address	21 Hume wood PE
Contact	0785256395
Physician	
Emergency Healthcare Contact	Dr Edward sekawabe 0785669658 family doctor
Emergency Family Contact	Eva ssozi 0739663258
Conditions	Allergies
05/08/2013 insomnia <i>can't sleep</i>	10/21/2000 general anesthesia <i>after surgery adverse reactions</i>
05/26/2013 migrame <i>took 6 panadol's</i>	05/28/1991 mushrooms <i>adverse reactions when taken</i>
	03/14/2004 penicillin <i>leads to anaphlaxis</i>
Medications	Medications (Other)
05/12/2012 paradox 4 4 twice a day	None.

Figure 3-6: Sample PHR from the Capzule mobile application

3.5.4 In Case of Emergency (ICE)

This application provides a critical functionality, it enables individuals to contact close relatives and medical practitioners in case of an emergency. The application can be configured to send out a SOS message (distress signal) including the GPS coordinates to select contacts.



Figure 3-7: Sample PHR from the ICE mobile application

This application can easily be accessed even from a locked smartphone. This comes in handy in case of an emergency but also risks exposing confidential information since anyone can easily access the information. The application does not display a privacy policy for users and also lacks basic security mechanisms such as login authentication.

3.5.5 Summary

The American Health Information Management Association maintains a listing of existing PHR applications categorised as either web-based, software-based or paper-based. A total of over 20 applications are listed in their directory (AHIMA, 2013). The goal is not to develop yet another

PHR application; rather it is to increase the probability of designing and implementing a successful PHR system. The compliance of the applications reviewed is presented in the next section.

3.6 Analysis of existing applications

PHR Applications:

- A. Microsoft Health Vault (MHV); B. HealthSpek
- C. Capzule PHR; D. ICE

Table 3-2: Compliance of PHR applications with the evaluation criteria (HealthSpek, 2013; Microsoft, 2013)

		A	B	C	D
#	Criteria				
1	Complete Data Elements	✓	✓	✓	✓
2	Providing everywhere access to personal healthrecords	✓	✓	✗	✗
3	Providing medical summaries for health care providers	✓	✓	✓	✗
4	Portal to patient-specific consumer-level health care information	✓	✗	✗	✗
5	Providing interpretive information about laboratory test and diagnostic study results	✗	✗	✗	✗
6	Serving as a database of information for patient-specific self-monitoring and disease management	✓	✗	✗	✗
7	Ensure data input accuracy (spell checking, reference data ranges)	✓	✗	✗	✗
8	Accept EHRs from medical providers	✓	✓	✗	✗

The data elements are supported by the four applications evaluated; this highlights the importance of having complete PHRs. Ubiquitous access to PHRs is supported by two of the reviewed applications, namely Microsoft Health Vault and HealthSpek. The provision of medical summaries to health care providers is supported by all applications except the *ICE* application. Apart from

Microsoft Health Vault, criteria (4-7) is not supported by HealthSpek, Capzule PHR and ICE. Microsoft Health Vault and HealthSpek provide support for accepting EHRs from medical providers. It was observed that whereas confidentiality is of utmost importance when handling medical records, Capzule PHR had no measures in place to ensure data privacy. Capzule PHR makes use of password authentication. HealthSpek makes use of the Secure Sockets Layer to transfer medical data between their servers and client mobile devices. HealthSpek also claim to have firewall services and data protection as well as follow the ISO 17799-based policies and procedure (ISO17799, 1992). Whereas the existing applications go a long way in addressing the needs of PHR management on mobile devices, more can be done to improve these applications. For example, making applications more PHR-specific and incorporating security mechanisms aimed at ensuring the confidentiality of information. Privacy policies can also be displayed so that potential users are better informed of the inherent risks involved in sharing health information online.

In order to support ubiquitous access to PHRs, a suitable underlying architecture needs to be selected. The next section discusses existing PHR architectures with the aim of identifying and motivating one for use in South Africa.

3.7 Existing PHR architectures

This section discusses the existing PHR architectures. The objective of reviewing information architectures is to motivate which type of architecture is best suited for mHealth applications in South Africa and in particular the ones concerned with PHR information management.

For the purposes of this research, an information architecture is defined as a component of an enterprise architecture that is concerned with the structural design of shared information environments. Both information and enterprise architectures fall under the systems design field (Dillon, 2002; IA, 2013; Mentz, Kotze, & Merwe, 2012). The information architecture category was chosen for this research because it partly describes how ubiquitous information access can be realised. Enabling ubiquitous access to PHR information is one of the objectives of this research.

Fong & Goldfine, (1989) argued that there is no single correct way to develop architectures for every enterprise. They concluded by stating that an architecture, must be customised to a given environment. They identified five components of any given architecture as: *business unit, information, information system, data, and delivery system*. A detailed explanation of the five components was not presented by the authors. However, Steele & Lo, (2012) extend the argument by Fong & Goldfine, (1989) and define a PHR architecture as an architecture that provides a description of how it addresses the storage, management and access of health data. It also provides descriptions of the hardware, software and networking components required for the delivery of data to allow for goals such as the enablement of on-demand access to data. Both definitions highlight the significance of the storage and management of information whilst taking into consideration the underlying hardware, software and networking components.

A given PHR architecture may imply different functional capabilities for community or nation-wide health care systems. Hence, it is important to objectively evaluate existing architectures before settling for one. One notable example is the use of *smartcard*-based PHRs in Europe and *web-based* PHRs in the USA (ABC, 2011; Clarke, Meiris, & Nash, 2006). The discussion that follows reviews the different categories of PHR architectures and motivates one, which is suitable for use in South Africa.

Steele & Lo, (2012) consider how available infrastructure impacts PHR architecture, functionality and benefits. Their classification is based on *connectivity coverage* and *ubiquitous technology baseline*, which are defined as:

- (i) Connectivity coverage: Impacts the physical location of the PHR data.
- (ii) Ubiquitous technology baseline: Deals with issues such as whether PHR storage devices are fixed or portable, the software/hardware requirements and the required web-based infrastructure.

Table 3-3: Classification of PHR architectures based on Connectivity and Technology (Steele & Lo, 2012)

Connectivity Coverage		Ubiquitous Technology Baseline	
PHR Architecture	Storage Device	Device and Software Requirements for Data Access	Web-based hardware
Local -Data locally available -No internet connectivity required	-USB -Smartcard -Mobile Phone	- USB interface and software - Card reader interface - PHR software	Not Applicable
Remote -Continuous internet connectivity required	-Web-based server -Cloud-based server	-Web-browser	-Remote web server -Remote dedicated server
Hybrid (Local and remote duplication) -Intermittent internet connectivity required	-Local devices and remote server	-Local PHR software and local computing device -Local web browser and internet connected computing device	-Remote web server

Table 3-3 demonstrates how various types of PHRs can be classified according to connectivity coverage and ubiquitous technology baseline. A discussion of PHRs under the categories of Connectivity coverage and Ubiquitous Technology Baseline follows.

3.7.1 Connectivity Coverage

Local PHR architecture

Data is predominantly stored on portable USB (Universal Serial Bus) devices, smartcards or mobile devices (Chaplin, 2007; Maloney & Wright, 2010; McClain & Thompson, 2010). Patients can use such devices to store and maintain their PHRs. The local PHR is characterised by the fact that network connectivity is not required and its data is portable as it is stored on a portable storage device. One limitation of the local architecture is that individuals are not able to access their records if they lose the physical storage device. This limitation rules out the possibility of using an entirely local PHR architecture since it does not help in addressing one of the research objectives concerned with everywhere access using different mobile devices.

Remote server-based PHR Architecture

The PHRs are stored on a web-based server possibly managed by a health care provider. Patients can store and maintain their PHRs via an internet connection, which could be classified as a tethered or interconnected PHR (Simons, Mandl, & Kohane, 2005). Whilst an internet connection will facilitate ubiquitous access to PHRs, under normal circumstances, this architecture requires individuals to be connected to the internet whenever they need to access their health records. This architecture will form part of the design.

Hybrid PHR Architecture

The Hybrid Architecture is a cross between local and remote PHRs; such PHRs allow data to be duplicated on both local storage devices and remote servers. This PHR is likely to provide better accessibility to data and withstand unexpected system and infrastructural vulnerabilities like natural disasters, network or power failures. The hybrid PHR Architecture is the most suitable for use in South Africa from the connectivity coverage classification since individuals are able to access their data regardless of whether they have an internet connection or not.

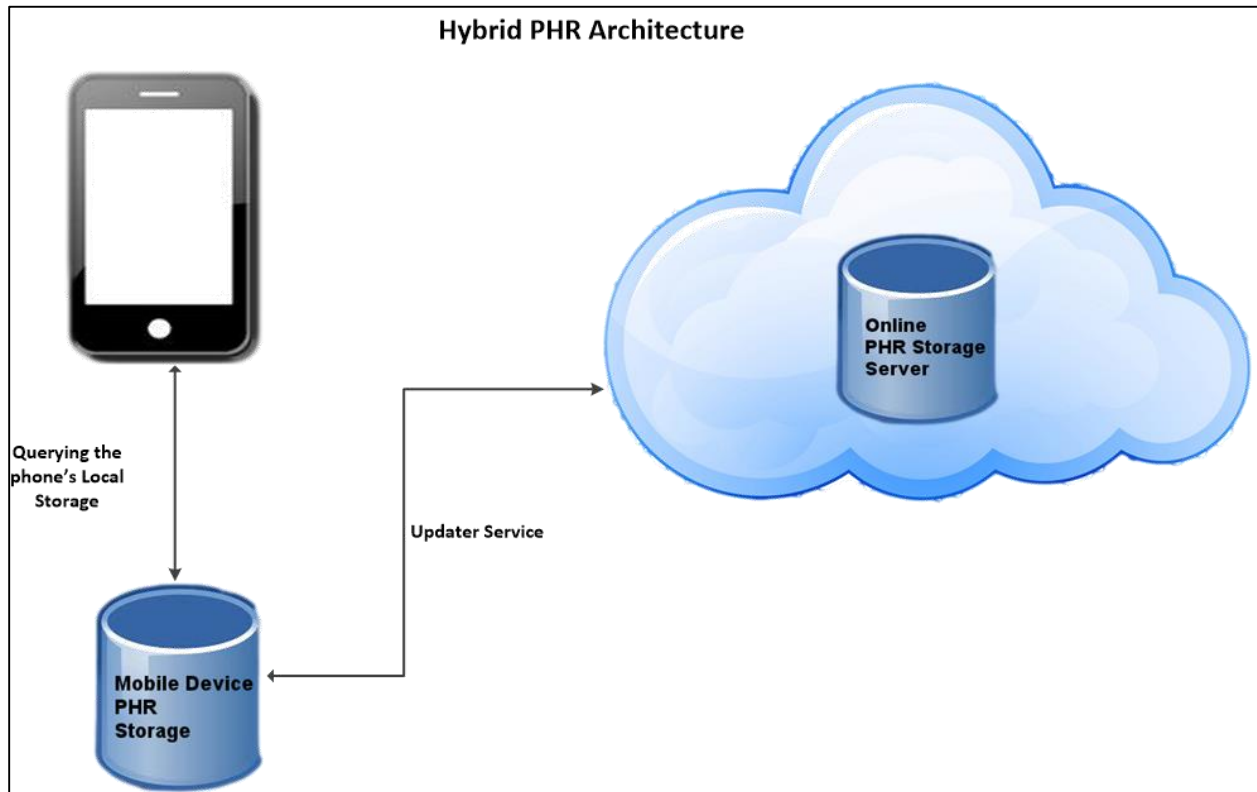


Figure 3-8: Hybrid Architecture, adapted from (Steele & Lo, 2012)

The next section discusses the ubiquitous technology baseline classification in order to understand the existing software/hardware that can be used to support the Hybrid PHR architecture.

3.7.2 Ubiquitous Technology Baseline

Card Reader Interface

The card reader interface involves the use of a smart card, which is used to store the data. This architecture is predominately used in Europe and it necessitates investments in technology to print the cards for individuals and card readers for whoever wants to read the stored medical record. The costs involved are not suitable for the smart card PHR architecture in South Africa. An architecture with minimal start-up costs and nationwide public acceptability for example mobile devices is more suitable.

USB Interface and Software

USB devices are cheap and readily available in South Africa and hence can make it easy for individuals to store their medical information. However, they can easily be misplaced and hence increasing the risk of exposing an individual's health information.

Web browser

A web browser on mobile devices would be ideal if people were always connected to the internet. Unfortunately, this is not the case hence the use of a web browser as the only means of accessing medical records does not cater for situations where an individual is not connected.

Local and Internet Connected Devices

This is ideal for ensuring ubiquitous access to medical information since individuals are able to access their information regardless of whether they are connected to the internet or not. Hence, local and internet connected devices together with the hybrid architecture are best suited for use in South Africa.

A discussion of the ubiquitous technology classifications has shown that the use of local and internet connected devices is ideal for South Africa since individuals are able to access their medical records with or without internet access. The use of a card reader interface is not suitable because the costs involved are higher than both the internet connected devices and USB interfaces. The USB interfaces were found to be not suitable because they can easily be misplaced hence increasing the chances of confidential medical data leakage or loss.

With the above mentioned classifications, PHR architectures with their functional and infrastructural implications were studied and analysed. The Hybrid PHR architecture was found to be best suited for use in South Africa. The next section compares the Hybrid PHR architecture with a slightly different cloud-based architecture named 'MyPHRMachines'. The comparison will motivate whether to adopt the Hybrid architecture for this research or incorporate some components from the cloud-based architecture deemed essential for use in South Africa.

MyPHRMachines Cloud-Based PHR System Architecture

The MyPHRMachines architecture was developed and presented by Gorp & Comuzzi, (2012). Their architecture involves care organisations, which generate health-related data, which may become relevant for other care givers. Figure 3-9 models a patient interacting with the MyPHRMachines portal. The PHR data of a patient is mounted on their virtual machine (VM). The supportive infrastructure should ensure that data is only mounted on VMs that have been started by the data owner. Using the portal, the patient can select, start and stop remote VMs to which the PHR data will be mounted securely. By default, MyPHRMachines blocks all traffic from a VM to the Internet; thus by default patients are assured that their sensitive data cannot be transferred to other internet locations during the VM execution.

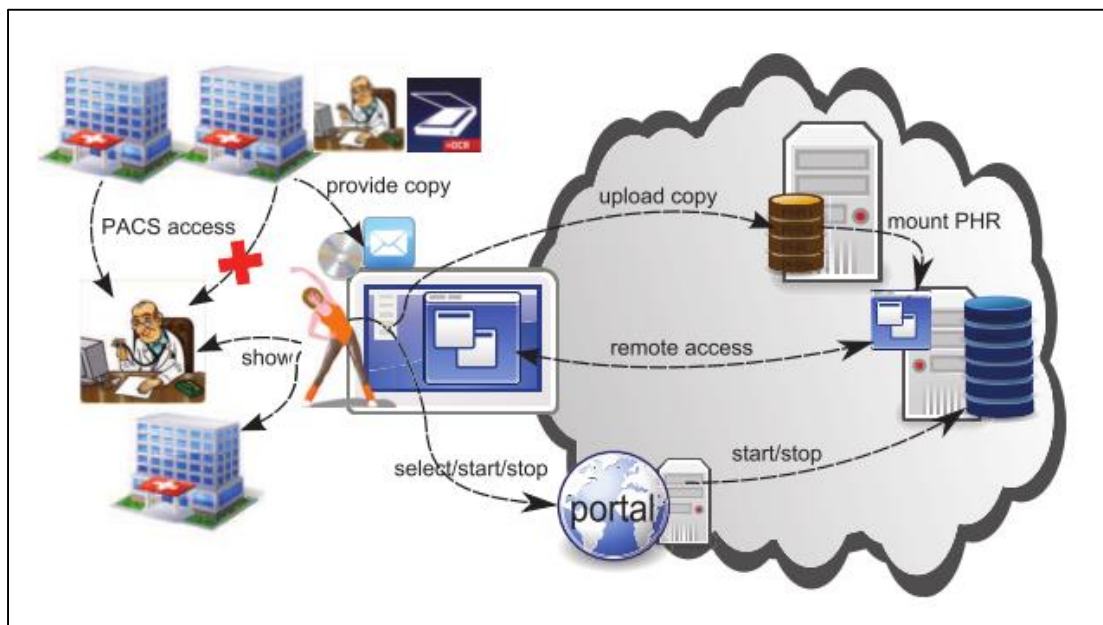


Figure 3-9: Cloud-Based PHR System Architecture (Gorp & Comuzzi, 2012)

The key functionalities of the system as described by the authors are:

- (i) Remote access to PHR data; that is patients can use a desktop web browser, a smart phone application, or any other device with appropriate internet access and display capabilities.
- (ii) Virtual machines can contain advanced decision support software, specialised medical viewers and data transformation software.

- (iii) The execution of application software is not constrained by the care giver device capabilities, since it occurs remotely in virtual machines.
- (iv) Sharing with General Practitioners: caregivers receive a unique URL that gives browser access to a running VM as long as the PHR patient keeps it running.

The MyPHRMachines architecture is made up of the following key components: Remote data storage hardware, networking components and End user software. Whereas the MyPHRMachines architecture does cater for security of health information by putting in place mechanisms to ensure the privacy of personal health information, the Hybrid PHR architecture does not consider the privacy of such information. Hence, the Hybrid architecture should be extended in order to ensure the privacy of medical information using mechanisms identified in Chapter 2.

Ubi-data architecture

Helal et al. (2001) propose a three tier architecture that addresses accessibility, availability and consistency of data in mobile environments (Figure 3-10).

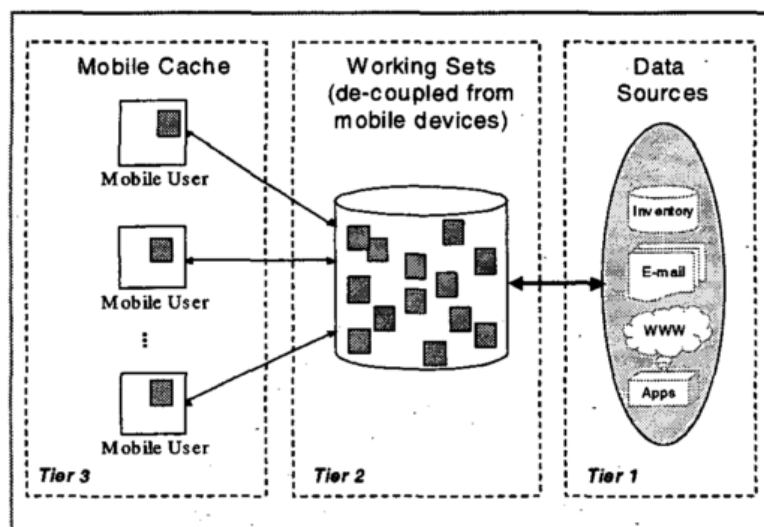


Figure 3-10: Three tier architecture, adapted from (Helal *et al.*, 2001)

The Three tiers are:

- (i) **Tier 1:** The data sources, which include but are not limited to file systems, database systems, database servers and web servers.
- (ii) **Tier 2:** The working set (one per user), which are decoupled from mobile devices.

(iii) **Tier 3:** The mobile caches, which contain copies of a subset of the user's working set.

The middle tier serves to separate the mobile nodes from the data sources, shielding each from the changes that have affected the others. The middle tier acts as mobility-aware persistent store. When the user is connected, it accumulates the user's working set. When the user is roaming, it collects updates affecting the disconnected users and keeps the user's working sets up-to date. When the mobile user returns, it synchronises the collected updates in the warehouse with the contents of the mobile cache.

The issues addressed in the three tier architecture are now also addressed in mobile operating systems such as Android and iOS (Android Team, 2012). It is possible that the work of Helal *et al.* and others led to the current seamless integration of such features into the modern operating systems. Abdelsalam & Hammer, (2004) also propose the Ubidata architecture that aims to address the issues of any-time and ubiquitous access as well as device and application independent data access. Their work describes algorithms that support automatic selection, filtering, hoarding and synchronisation of data and files across platforms and applications, user profile and metadata management, and support for mobile transactions.

3.8 Conclusion

The aim of this chapter was to answer research question RQ2: *What are the strengths and shortcomings of existing mHealth Systems that can be used to support the management of PHRs?* This chapter achieved this objective by reviewing existing mobile health (mHealth) systems and architectures that can be used to support ubiquitous access and secure sharing of PHRs.

The chapter started off with a classification of the existing mHealth applications; this helped highlight the existing gaps in personal health information management and illustrate how this research intends to address these gaps. A review of existing PHR applications was carried out using a predetermined set of criteria. It was determined that whereas most of the applications adhere to the PHR data elements, features meant to ensure the confidentiality of the data and enhancing the usability of PHR applications need to be improved. Apart from Microsoft Health Vault, the applications reviewed lacked features to ensure data input accuracy. Privacy policies,

which are intended to educate users as to the risks involved in storing their medical data online, were also absent.

A review of the existing PHR architectures was conducted. The architectures were classified either under the Connectivity category or the Ubiquitous Technology classification, which is concerned with the underlying technologies used. The hybrid PHR architecture was found to be the most suitable for use in South Africa since individuals are able to access their records whether they are connected to the internet or not. Under the ubiquitous technology category, smart card technology was found to be expensive due to the start-up costs involved. USB drives were found to be insecure since they can easily be misplaced. Mobile devices were found to be the most suitable since they are widely available in South Africa.

This chapter has explained existing evaluation criteria for PHRs, identified shortcomings of existing applications and identified the Hybrid PHR architecture as the most suitable for use in South Africa.

The next chapter proposes a PHR management model that addresses these shortcomings. The proposed model makes use of the hybrid PHR architecture identified in this chapter and the PHR information management requirements that were identified earlier in Chapter 2.

Chapter 4: Hybrid PHR Management Model

4.1 Introduction

The objective of this chapter is to present the design of a model that facilitates ubiquitous access and secure sharing of PHRs in South Africa. The proposed model is an adaptation of the Hybrid PHR architecture discussed in Chapter 3. The Hybrid PHR architecture stores PHR data in a cloud environment and on local devices. The main limitation of the Hybrid PHR architecture is that the data stored in a cloud environment is not secured.

The CP-ABE, which was discussed in Chapter 2, is used to ensure fine grained access control to PHRs. A discussion of the CP-ABE as used in this research is provided later in this chapter. Chapter 2 also discussed the functional and data requirements of PHRs in South Africa. These requirements were identified through a literature review. Section 4.2 discusses the findings from interview studies that were carried out with three medical practices in Port Elizabeth. The interview studies were carried out in order to contextualise the PHR functional and data requirements.

The design of the Hybrid PHR Management model is discussed in Section 4.3. The design of the system is discussed in Sections 4.4.

Section 4.5 discusses the implementation details of the two applications; a mobile application for patients and a web application for medical providers. The mobile and web applications were developed as a proof of concept. This chapter answers Research Question 3 (RQ3): *How can a model be designed and prototype applications implemented to support personal health management?*

Section 4.6 discusses the findings from an expert review of the system. These findings were used to improve the usability of the system prior to evaluation.

4.2 Interview Studies

The aim of the interview studies was to understand how medical records are currently managed in South Africa and how medical practices can make use of PHRs. Emphasis was put on small practices. The functional and privacy requirements of PHRs that were considered during the interview study were taken from the international PHR System standard by HL7 discussed in Section 2.5.2. The aim was to contextualise the PHR data elements identified in Chapter 2 for use in South Africa. The data elements considered were: allergies, immunisations, surgeries, chronic conditions, medications, family history and imaging.

The interview questions were:

- (i) Explain how you currently manage your patient medical records.
- (ii) What challenges are you facing in relation to managing patient medical records?
- (iii) What is the process that you use when you get a new patient?
- (iv) Do you think this process could be improved?
- (v) What is your opinion on patients having an electronic copy of their medical records?
- (vi) Which of the PHR data elements do you currently capture and why?

Participants from two medical practices and a student medical centre at a local university were interviewed. For confidentiality purposes, the medical practices are referred to as Medical Practice A and Medical Practice B.

4.2.1 Medical Practice A

A medical doctor at Medical Practice A was interviewed. The practice stores patient data in paper files and a spreadsheet is used to cross-reference files. The administrative users find the filing system easy and manageable. The spreadsheet contains patient contact data, insurance data and file look up information, while paper files contain the actual medical records. The data is entirely managed by an administrative assistant who is tasked with capturing details and filing. The doctor is not involved with filing patient medical records. The doctor records medical details of the patient onto paper, which is then passed onto the administrative assistant for filing. The doctor was open to the idea of having a copy of a patient's medical history presented to him by a patient either in

paper or electronic format. However, the doctor was not open to the idea of having to enter the medical details into a computer or mobile device as this would take up his time.

The doctor motivated the need for the following PHR data elements:

- (i) **Allergy Data:** If a doctor prescribes a drug and the patient develops an allergic reaction to it, a subsequent doctor may not know about the allergy. In order to prevent more harm to the patient, such data should be made available.
- (ii) **Immunisation Data:** Repeating vaccines makes them ineffective and they are also expensive.
- (iii) **Operational Surgery Data:** For example, if a patient has had gall stones removed in the Eastern Cape and she shows up elsewhere with the same symptoms, the doctor should not consider gall stones as a possible diagnosis.
- (iv) **Chronic Condition Data:** Patients may have chronic prescription scripts, such as for diabetes or hypertension. There is a need to keep that information to ensure continuity of care.
- (v) **Medication Data:** Doctors need to know what kind of medication a patient has been taking.
- (vi) **Family History:** A patient's family history can help a doctor in diagnosing an ailment.
- (vii) **Imaging Data:** The X-ray department sends the doctor medical images, which is considered to be convenient.

The doctor also highlighted the importance of the privacy of medical records. Their medical data is stored in a locked wall filing cabinet.

4.2.2 Medical Practice B

An administrative clerk at Medical Practice B was interviewed. Medical Practice B is a small sized medical practice with one general practitioner and a dentist. The practice stores its patient data in paper files. A file is opened for each new patient. The files are managed by the administrative clerk. The practice currently captures the following PHR data elements:

- (i) Allergy data.
- (ii) Immunisation data.
- (iii) Operational surgery data.
- (iv) Chronic condition data.
- (v) Medication data.

- (vi) Family history data.
- (vii) Imaging data.

The practice reported being open to the idea of patients having an electronic copy of their medical records. However, they were concerned about safeguarding the privacy of the patient data. The data is stored in physical files.

4.2.3 Student Medical Centre

A medical administrative clerk at the student medical centre was interviewed. The centre provides the following services to their students: primary health care, occupational health services and HIV and Aids services. The medical centre stores student medical data in paper files. The centre currently captures the following PHR data elements:

- (i) Immunisation data.
- (ii) Operational surgery data.
- (iii) Chronic condition data.
- (iv) Medication data.
- (v) Family history data.
- (vi) Imaging data.

However, the centre faces a problem of not having access to student medical histories. Few students are able to provide this information, which the centre deems essential for continuity of care. The medical administrative clerk welcomed the idea of students having electronic copies of their medical records. The medical administrative clerk highlighted the need to have access to these records from desktop computers rather than mobile devices. He was also concerned about electronic medical records being accessed by unauthorised persons because this could violate the privacy of their patients. The medical administrative clerk shared an unpleasant experience with an EMR system that was procured for the centre. He emphasised the need of having a simple system that is easy to use and learn. The EMR system is no longer in use at the centre.

4.2.4 Summary of findings

The three practices have processes in place that enable them to adequately manage their patient medical records. However, it was observed that none of the practices could share medical records amongst themselves. The patient would have to physically request a copy of his/her medical records and take the copy to a different medical practice. One way of addressing this is by empowering patients to be actively involved in the management of their medical records.

Medical practices would like access to complete medical histories of their patients. However, the patient should have little or nothing to do with the actual management of their records. It was also noted that medical doctors should not be tasked with entering medical data for patients as this can waste their valuable time. However, they can be presented with an electronic copy of medical data. This information should be presented using desktop computers as this caters for the doctors' context of use. The next section discusses the design of the Hybrid PHR Management Model. The model design takes into consideration the context of use of medical care providers.

4.3 Model Design

This section discusses and adapts the Hybrid PHR architecture from Chapter 3 (Steele & Lo, 2012). A description of the encryption approach used and the motivation is then provided and lastly the adapted Hybrid PHR architecture is presented.

4.3.1 Hybrid PHR Architecture

The Hybrid PHR Architecture was chosen as the most suitable because:

- (i) It facilitates both remote and local file storage; and
- (ii) It does not rely on external hardware like card readers.

However, the Hybrid architecture has a major limitation: The privacy of data in the Hybrid architecture is not guaranteed. Storage service providers can gain unauthorised access to stored data. Section 4.3.2 describes the encryption approach and mechanisms the proposed model uses to ensure that privacy is not dependent entirely on trust.

4.3.2 Encryption Approach Used

The CP-ABE was introduced in Chapter 2. Figure 4-1 below illustrates the CP-ABE encryption approach. Only users whose secret key attributes have been added to the access policy specified

in an encrypted file can decrypt the given file. For example, Bob, Sarah and Peter have their secret keys added to the access policy while Eva's secret key is not added. This implies that Bob, Sarah and Peter can decrypt the encrypted file while Eva cannot decrypt the file.

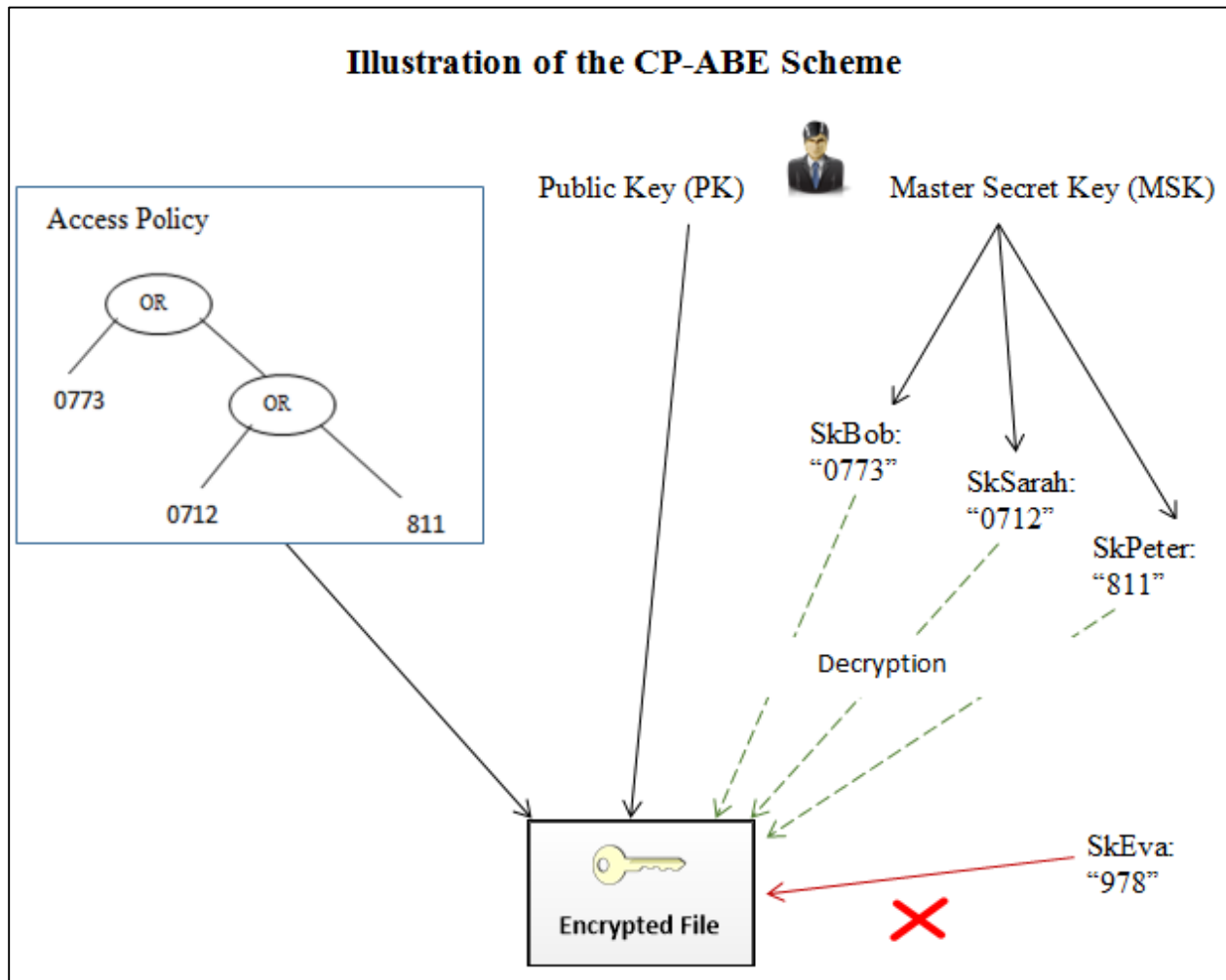


Figure 4-1: Ciphertext Policy Attribute Based Encryption (Bethencourt *et al.*, 2007)

The advantages of CP-ABE are:

- (i) Files are encrypted before being stored on third party servers.
- (ii) Setting up keys is offline
- (iii) No online, trusted party mediating access to files or keys
- (iv) Highly expressive, fine grained access policies

The next section presents the Hybrid PHR Management Model. The model was developed as a result of the culmination of the review on Personal Health Information Management (Chapter 2) and Mobile Health Applications and Architectures (Chapter 3).

4.3.3 Hybrid PHR Management Model

Yarbrough & Smith, (2007) carried out research on technology acceptance amongst physicians and noted that physicians were hesitant to adopt new technologies because of the following issues, amongst others:

- (i) The filling out of computerised entry forms took up more time as compared to paper forms.
- (ii) The perceived benefits of IT were not very clear to the medical practitioners.

Koehler *et al.*, (2013) carried out a study in Australia to enumerate the number of healthcare professionals who use mobile phones in clinical practice and their attitudes towards using them. Healthcare professionals were found to have more positive attitudes towards internet compared to mobile phone usage in clinical practice. Healthcare professionals also had the perception that patients may think that mobile phones were being used for non-medical purposes.

The findings from the interview study in Section 4.2 further highlight the need to cater for the context of use of medical doctors. That is, desktop computers are preferable to mobile devices. The Hybrid PHR management model illustrated in Figure 4-2 below takes this into consideration.

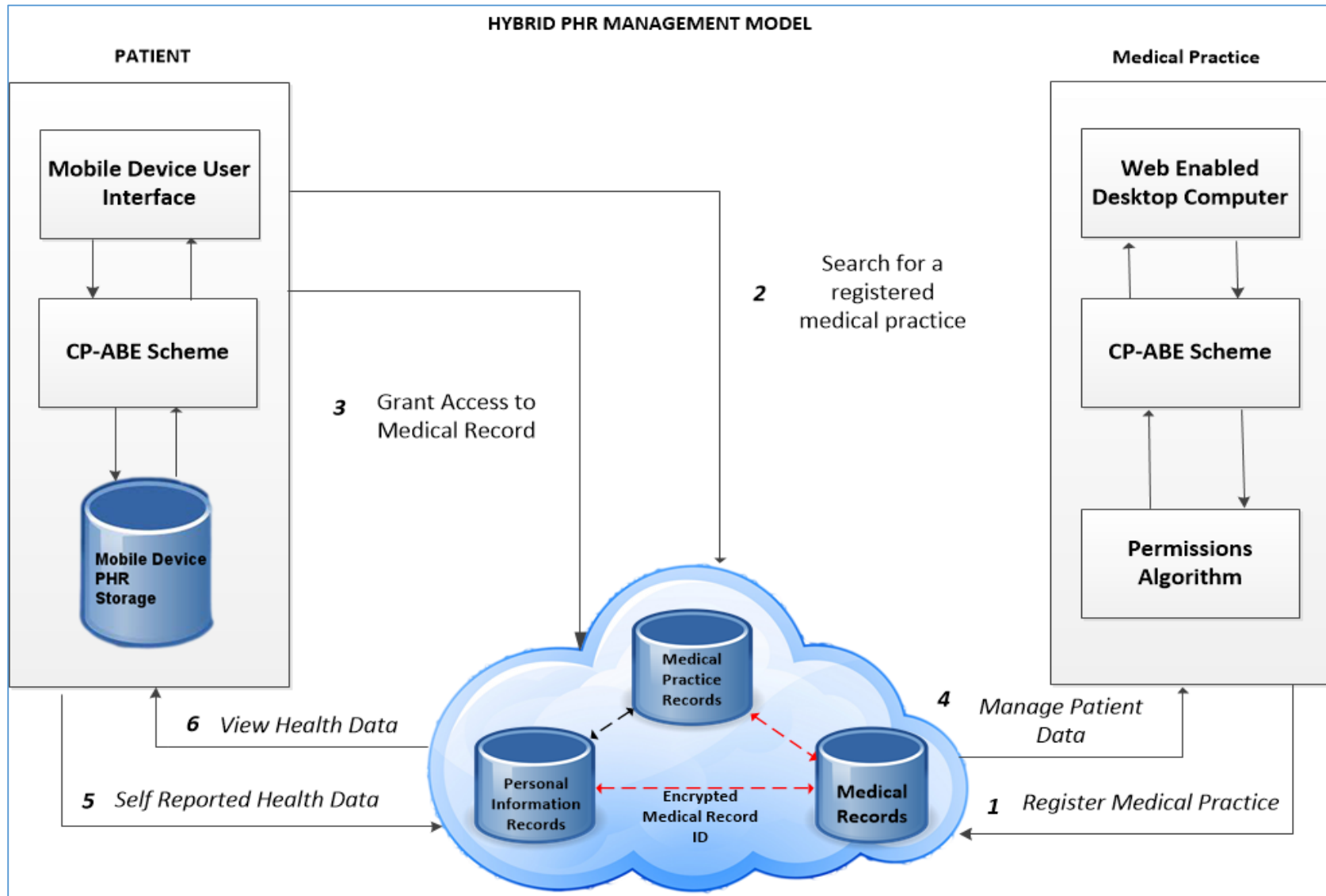


Figure 4-2: Proposed Adaptation of the Hybrid PHR Architecture

The model in Figure 4-2 is explained in detail below:

Mobile Device User Interface

This component allows individuals to search and connect the various medical practices from, which they receive care. Each of the connected medical practices has access to a given patient's complete medical record.

CP-ABE Scheme

This is an implementation of the Cipher Text Attribute Based Encryption Scheme as described in Section 2.3.3 and illustrated in Figure 4-1. The implementation details are specified in Section 4.5.

Desk Top User Interface

The Desk Top User Interface component is designed for physicians.

Permissions Algorithm

The permissions algorithm (described in Appendix D) ensures that medical practices can only access those sections of a medical record, which they are permitted to. The use of two different data stores allows the easy separation of personally identifiable information from the medical information. Each PHR owner will have two documents, one containing their personal information and an encrypted medical id field and the other containing medical information. This separation will have the following benefits:

- (i) An individual's privacy will be ensured.
- (ii) The medical information may be used by third party researchers without the possibility of linking it back to the owner.
- (iii) The encryption workload will be greatly reduced since only the medical id field in the person details collection needs to be encrypted.

On successful decryption of the medical id, medical practice personnel will only be able to view authorised medical information as specified in the permissions algorithm in Appendix D.

4.4 System Design

The three tier model divides an application into three distinct sections, namely a business logic section, a data section and an interface section. The model has been shown to be successful in creating extensible and flexible applications (Steiert, 1998). This section discusses the functional, data and interface design of the PHR system.

4.4.1 Functional Design

Figure 4-3 illustrates the use case of the ubiquitous PHR Management System. The two actors are the patients and medical personnel. The medical personnel are related to medical practices. Patients are tasked with linking their accounts with their medical care providers. Medical care providers are tasked with creating, reading and updating of their patient records. Patients can contribute to their health record by self-reporting medical conditions.

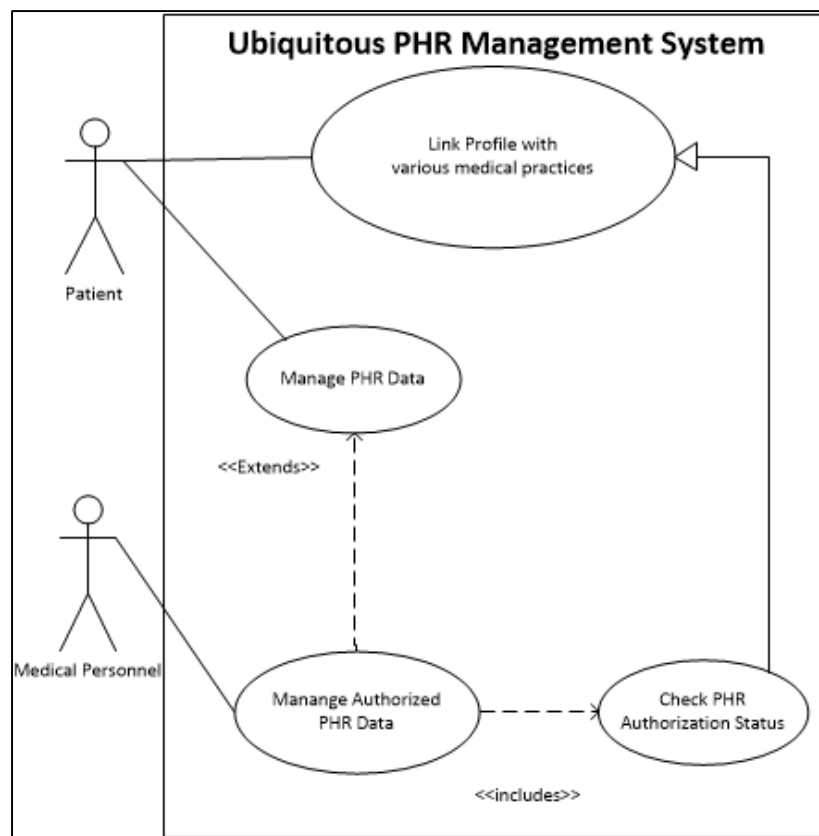


Figure 4-3: Use case diagram for PHRs

4.4.2 Data Design

The main data elements of a PHR were listed in Table 2.2. Section 2.6.1 described HL7's PHR standard, which was chosen for this research. A summary of the functions is provided below

- (i) PH.1 (Account Holder Profile): Manage PHR Account Holder demographics, preferences, Advance Directives, consent directives and Authorisations.
- (ii) PH.2 (Manage Historical Clinical Data and Current State Data): Historical health information as well as current health status should be captured and maintained in the health record.
- (iii) PH.6 (Manage Encounters with Providers): Manage information for scheduling, preparation, and assimilation of knowledge gained by encounters with providers.
- (iv) IN.1 (Health Record Information Management): Capture, store, secure, message, display and report PHR information across PHR applications.
- (v) IN.3 (Security): Secure the access to a PHR application and PHR information

A UML class diagram represents a static view of an application. It describes the attributes and operations of a class and also the constraints imposed on the system. Figure 4-4 illustrates the UML class diagram for the PHR model. The class names and attributes are contextualised for South Africa. For example, see the replacement of the term “*Insurance*”, which is used in the international PHR standard with “*Medical Aid*”, which is commonly used in South Africa.

The South African ID number was chosen as the patient identifier for the PHR system. The ID number was chosen over a telephone number because every South African has one unique ID as compared to several telephone numbers.

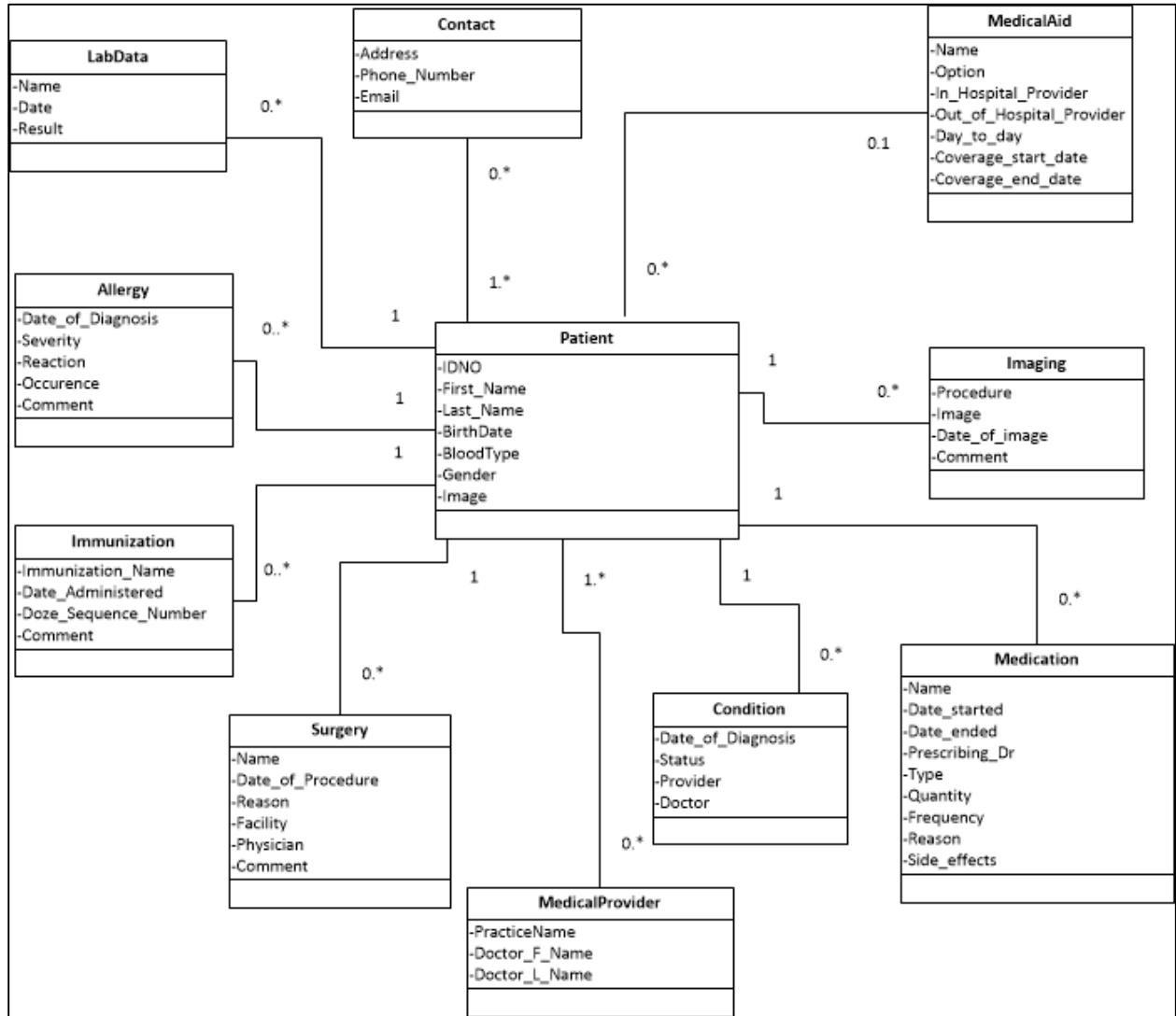


Figure 4-4: PHR UML Class Diagram

4.4.3 Interface Design

The interface designs are illustrated in Figures 4-5 and 4-6 below. Figures 4-5 and 4-6 are screen designs of the Android mobile application. Android design patterns, such as the dashboard layout and the navigation drawer, were used. The use of design patterns ensures that the mobile application users can easily use the developed application.

Users are required to sign in into the application before they can access their health information (Figure 4.5). However, a remember feature is also integrated into the application so that users do not have to sign in every time that they want to access their data. Once users have signed into the application, they are able to perform the following (Figure 4.5):

- (i) Create, Read, Update and Delete their self-reported health data
- (ii) View their consultation data
- (iii) View their medication data
- (iv) Search for medical care providers and connect their accounts with a given medical care provider.

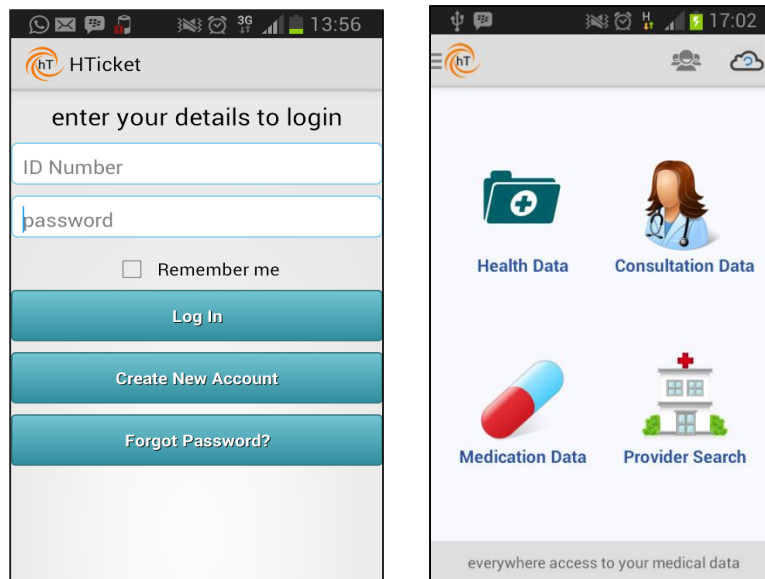


Figure 4-5: Login and Home Screens

Figure 4-6 illustrates the search results of a given medical care provider. A user can then connect his/her profile with the selected medical care practice by first setting data access permissions for the medical care practice.

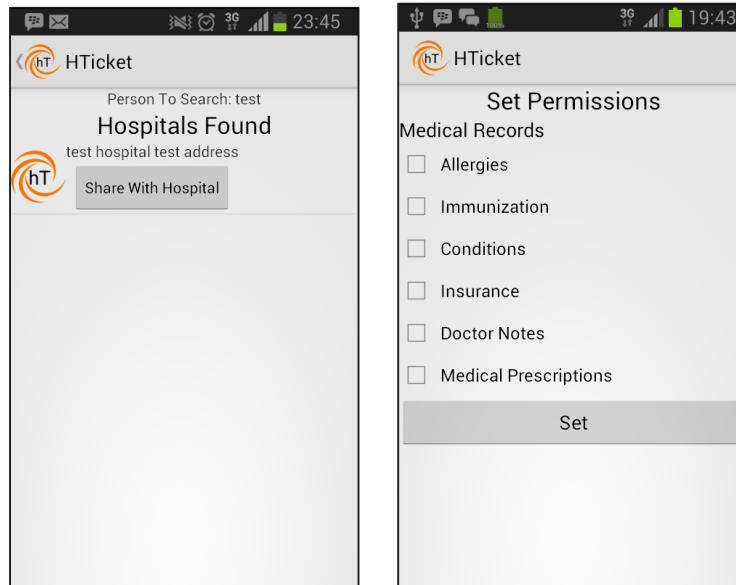


Figure 4-6: Search Results and Permissions Screen

Web Application

The web application was developed for physicians/medical care providers. Figures 4-7 and 4-8 illustrate the screen designs of the web application. A medical care provider can search for their patients (Figure 4.7). Once a patient is selected, medical providers can view their health records and update them as needed (Figure 4.8). The medical care providers can also register their medical doctors and personnel on the web application. A medical care provider's attention is drawn to the patient search feature because of the large font size.

Once a patient is selected, three tabs are presented namely:

- (i) Patient generated: Displays a patient's self-reported health data.
- (ii) Doctor input: Enables a doctor to add consultation notes and also view consultation notes by other medical care providers.
- (iii) Image Files: Enables a doctor to add medical image files and also view medical image files uploaded by other medical care providers.

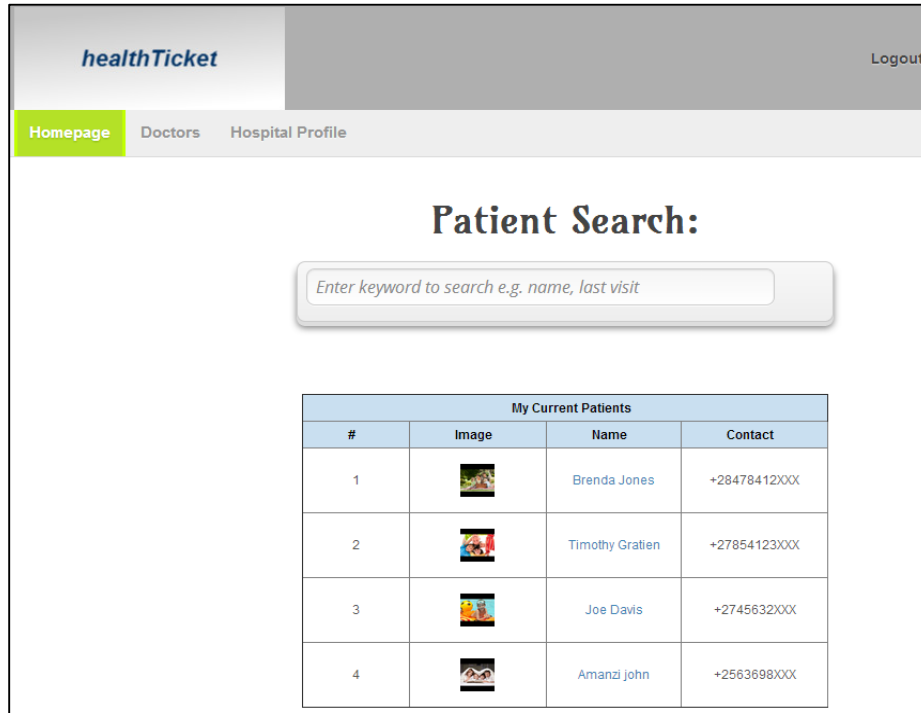


Figure 4-7: A sample list of patients connected to a medical practice

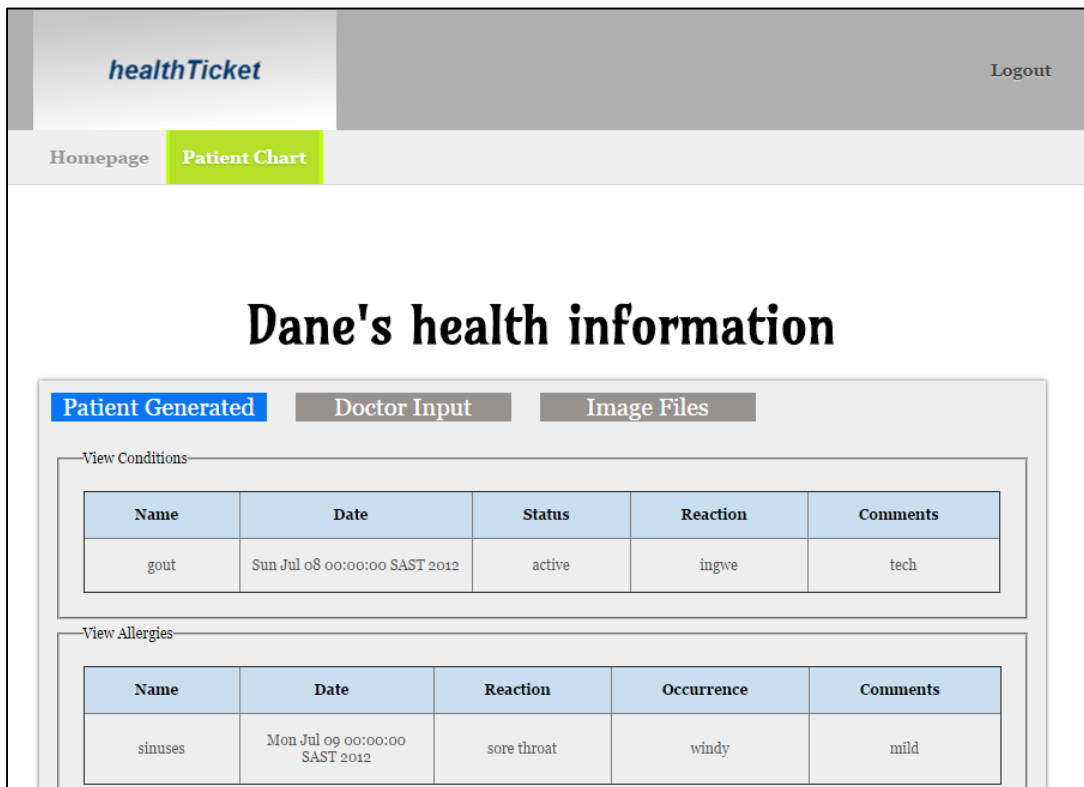


Figure 4-8: Sample patient chart

4.5 Implementation

The implementation was undertaken to demonstrate whether the model can be effectively used to implement a PHR system. This implementation partly answered research question **RQ3**: *How can a model be designed and prototype applications implemented to support personal health management?* The implementation tools selected to develop the prototypes are discussed. The implementation details of the mobile application and the web-based system are discussed in Sections 4.6.2 and 4.6.3 respectively.

4.5.1 Implementation tools

Different aspects of the model required the use of different development tools. The system was consequently implemented using the tools discussed.

Web Application technologies – A deployed web application can be accessed from any internet connected device; therefore, the implementation language of the web application is not of great concern. The web application was developed using Java and run on an Apache Tomcat Server. The application was hosted on OpenShift, which is a platform as a service. The OpenShift platform provides the following core benefits (OpenShift, 2014):

- (i) Application auto scaling.
- (ii) System administration by Red Hat.
- (iii) A wide range of tools for developers. The tools enable easy deployment of applications from a development machine to the OpenShift cloud.

Mobile Application Platform – The mobile application was developed for the Android platform. This is because of the easy access to a wide range of Android devices, which are essential for evaluation purposes.

Cloud Storage Database – There are various cloud storage technologies which can be used to implement the Hybrid PHR Management Model. MongoDB was used as the cloud database and Mongolab.com as the cloud storage provider. The discussion below provides an overview of cloud computing and cloud storage in particular and motivates the choice made for this research project.

Defining cloud computing in the context of data storage services

There are several definitions for “cloud computing” and generally, they point at taking applications and running them on infrastructure other than your own (Chun, 2012). Cloud computing is categorised into three different service levels as illustrated in Figure 4-9.

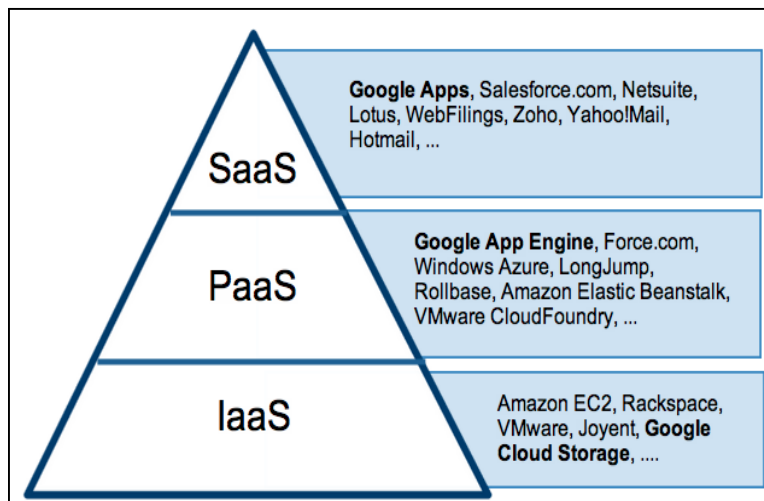


Figure 4-9: Cloud computing, adapted from (Chun, 2012)

The three service levels in Figure 4-9 are defined as:

Software as a Service (SaaS): SaaS refers to the end user programs accessed over the internet and hosted by cloud providers

Platform as a service (PaaS): With PaaS, the hardware, the underlying operating systems and software are installed and managed by third parties. Software developers can utilise provided software components, such as a database backend, and build their applications on top of the PaaS

Infrastructure as a service (IaaS): IaaS is concerned with utilising virtual hardware, i.e. the hardware is maintained by a third party. The person who utilises this hardware is tasked with installing the operating system and managing all the administrative tasks associated with physical machines.

The information storage needs of this research can be categorised under the PaaS category. The aim is to leverage existing third party database services. This will provide the following benefits:

- (i) Save hardware costs since there is no need to purchase hardware.
- (ii) System administration tasks are carried out by third parties.
- (iii) Easily scale data storage with user growth.
- (iv) Guaranteed uptime.

This section has defined mobile computing in the context of data storage services. The different cloud computing service levels were discussed and it was determined that the needs of this research fall under the PaaS category. The advantages of using this category were also discussed. The next section reviews the existing cloud storage services that can be used to achieve the goals of this project. The review will begin by identifying the desired features of a good cloud service and these will guide the evaluation of the technologies.

Cloud storage services and backup

Cloud storage services aim to provide uninterrupted access to data. The data requirements for PHRs were discussed in Chapter 2. The summary of the desired features of any given cloud storage service as illustrated in Table 4-1 were derived from the PHR data requirements. These features guide the evaluation of the various cloud storage services.

Table 4-1: Desired features of a PHR cloud storage service

Desired features
1) Ability to access the stored data at any given time
2) Ability to backup data with minimal effort from the consumer
3) Dynamic data schema: The schema should be flexible enough to cater for all patient records. For example, a patient without lab results should not have empty records in the lab results table.

Relational vs NoSQL Database Solutions

Traditionally, the obvious platform for most database applications has been a relational database management system such as Oracle or MySQL. However, the “*one size fits all*” approach for storage needs can no longer satisfy the needs of mobile and cloud computing (Stonebraker, Abadi, Harizopoulos, & Helland, 2007). Various types of applications have emerged, which have made database technology more demanding in various aspects. Some of the aspects are discussed below (Jing, Haihong, Jian, & Guan, 2011):

- (i) **High scalability and high availability:** With the increasing number of concurrent requests and data, the database needs to be able to support easy expansion and upgrades, and ensure rapid uninterrupted service.
- (ii) **Slow reading and writing:** With data sets, relational databases are prone to deadlocks and other concurrency issues, which can lead to a decline in the efficiency of reading.

Relational databases offer a rich set of functionality, these include; joins, transactions and strict schemas. However PHR applications may require a dynamic schema to cater for the variation in user data. This may not easily be achieved using relational database systems

To solve the issues discussed, a variety of new types of databases have appeared. These are referred to as "NoSQL" database systems. NoSQL is also interpreted as the abbreviation of "NOT ONLY SQL" to show the advantage of NoSQL. For the purposes of this research, NoSQL is defined as a database system, which is distributed, may not require fixed table schemas, usually avoids join operations, typically scales horizontally, does not expose a SQL interface and may be open source (Agrawal, Ailamaki, & Philip, 2008).

It is important to classify some products, which are categorised as NoSQL, as this helps us compare the different products and decide on, which one to use based on our research needs. Whilst there is no official taxonomy for this kind of software, several attempts do exist. Some of these attempts are discussed below (Stefan, 2013; Tudorica & Bucur, 2011):

Table 4-2: Core NoSQL Systems, adapted from (Stefan, 2013; Tudorica & Bucur, 2011)

Category	Examples
Wide Column Store	HBase and Amazon SimpleDB.
Document Store	CouchDB and MongoDB
Key Value / Tuple Store	Azure Table Storage and Redis
Eventually Consistent Key Value Store	Amazon Dynamo and Voldemort

Wide Column Store, Document Store

The categories specified in Table 4-2 may not adequately portray the entire landscape of NoSQL systems; rather they highlight the categories that can satisfy the data storage needs of this research. The document store category is the focus of this NoSQL review since each individual's health record is stored as a single document rather than a collection of scattered information in relational tables. Some of the advantages of document databases are:

- (i) Documents (objects) map nicely to programming language data types.
- (ii) Embedded documents and arrays reduce the need for joins.
- (iii) Dynamic schema makes polymorphism easier.
- (iv) Data access pattern is modelled according to the application needs (Lerman, 2011).

Both MongoDB and CouchDB are document databases that offer the functionality described in Table 4-3:

Table 4-3: Functionality of MongoDB and CouchDB (Apache, 2005; MongoDB, 2009)

Functionality	Details
High Performance	<ul style="list-style-type: none"> (i) Embedding makes reads and writes fast. (ii) Indexes can include keys from embedded documents and arrays. (iii) Optional streaming writes (no acknowledgments).
High Availability	<ul style="list-style-type: none"> (i) Replicated servers with automatic master failover.
Easy Scalability	<ul style="list-style-type: none"> (i) Automatic sharding distributes collection data across database servers. (ii) Eventually-consistent reads can be distributed over replicated servers.

Whilst both MongoDB and CouchDB can adequately address the data needs of this research, MongoDB was chosen due to the mature level of support in the industry and the easy access to third party MongoDB storage APIs. A real world case study of how MongoDB has been used to store electronic health records is presented below highlighting the benefits the developers realised by utilising a document database with health records.

MongoDB Industry Case Study

New wave telecom and technologies Inc. is a company, which has been supporting federal Healthcare programs for several years with some of its notable customers being the US department of Health and Human services amongst others. New wave technologies have used MongoDB to store electronic health records. According to Munis (2012), some of the benefits they realised include:

- (i) MongoDB provides a convenient, powerful and robust way to store structured/unstructured data.
- (ii) Leveraging of MongoDB's GridFS to store large files.
- (iii) Easily integrates with Hadoop to analyse data from local and external stores using Map/Reduce framework in Mongo.

4.5.2 Mobile Application

An Android mobile application was developed for the patients. The application uses SQLite for local phone storage. MongoDB (JSON document store) is used as the cloud database (MongoDB, 2009).

The participants accepted the terms and conditions before registering on the mobile application. The terms and conditions specify how the health information is stored. A login screen ensures that only the data owner can access their records. The home screen lists the various functionalities, which are:

- (i) Health data: Individuals can contribute to their health record by self-reporting medical conditions.
- (ii) Consultation Data: Individuals can access a view only version of their medical consultation record or their dependents' medical records.
- (iii) Medication Data: Individuals can access a view only version of their medication record or their dependants' medical records.
- (iv) Dependants Data: Individuals can contribute to the medical records of their dependants.

The mobile and web applications use the CP-ABE and depersonalisation of medical information as mechanisms to ensure that the privacy of individuals is guaranteed. The CP-ABE scheme was chosen because an individual can use their public and master private keys to generate restricted private keys for medical practices. The private keys have attributes. The individual can revoke a medical practice's access by removing the practice's attribute from a predefined access policy and re-encrypting the given object.

The CP-ABE's Setup algorithm is run on the mobile devices of patients. The algorithm generates a public key (PK) and master key (MK) for the patient. When a patient links their account to a medical practice, the CP-ABE's key generation algorithm is used to generate a private key (SK) for the given medical practice. The selected practice's email address and the MK are passed as the arguments to the key generation algorithm. The practice's email address is also added to the access policy (A). Encryption of medical record identifiers is done on the phone and the resultant

ciphertext is uploaded to the cloud. The encryption algorithm takes the following arguments: patient public key, message to encrypt and the access policy (A). The CP-ABE decryption algorithm is run on a server. The medical practices are able to decrypt the medical record identifiers using their patient generated private keys. An individual is able to search for a given medical practice and selectively grant and revoke access to their medical data.

4.5.3 Web Application

A Java web application was developed. The web application connects to the same MongoDB server as the mobile application. The web application provides medical practices access to the medical records of all the patients who have explicitly connected to them.

When a medical practice selects a given patient, the patients Public Key (PK) and encrypted medical record id (.cpabe file) are retrieved. Using the medical practice's secret key (SK), and the given patients public key, the medical provider is able to decrypt the (.cpabe file) and retrieve the medical id. The medical practice can then manage the patient's medical record using the permissions algorithm specified in Appendix D.

4.6 Expert Review

The design and implementation of the prototype applications followed an iterative process. An expert review was conducted in order to identify usability issues and improve the prototypes before commencing with evaluations.

Heuristic evaluations are carried out by experts with a goal of identifying usability issues of a given system (Bertini, Gabrielli, & Kimani, 2006). One of the benefits of heuristic evaluations is that usability issues can be identified early during development. The experts were given tasks that were to be performed by patients and medical practice participants. A description of the usability issues that were identified and corrected is given below.

Mobile Application

- (i) Splash screen: The mobile application displayed a splash screen on start up. The splash screen was removed. This made the application load faster.

- (ii) Search functionality: Searching for medical practices is a key feature of the mobile application. The application used the default Android search bar located at the top of the mobile phone. The search functionality was placed on the main dashboard. This made the feature more prominent and easy to find.
- (iii) Labels and icons: The application had some confusing icons. The icons were changed after the expert review.

4.7 Conclusion

The aim of this chapter was to partly answer Research Question R3: *How can a model be designed and prototype applications implemented to support personal health management?* This chapter achieved the objective by designing a model to facilitate ubiquitous access and secure sharing of PHRs and implementing a prototype application as a proof of concept.

The chapter started off with a discussion of the hybrid architecture from Chapter 3, which highlighted the security shortcomings of the architecture. The security shortcomings were addressed by the CP-ABE encryption mechanism. Authentication and depersonalisation of medical health data were also used to ensure patient privacy. For the mobile application, the patients are required to first accept the terms and conditions before they can register. This ensured that the patients make an informed decision as regards to the storage of their medical health data. The Hybrid PHR Management Model was then presented and discussed. The functional, data and interface design of both the mobile and web applications were discussed. The implementation tools and details were also discussed in detail. The technologies used are: the OpenShift platform for hosting the web application and the MongoLab database as a service easily integrate with each other. This greatly reduced the time spent on development of the applications. The next chapter discusses the evaluation of the prototype applications.

Chapter 5: Evaluation

5.1 Introduction

The objective of this chapter is to evaluate the effectiveness and usefulness of the prototype mobile and web applications implemented in Chapter 4. Specifically, the chapter seeks to answer Research Question 4 (RQ4) How usable and effective are the prototypes designed to validate the proposed model? The prototype applications were implemented as a proof of concept of the Hybrid Personal Health Record Management Model. Chapter 4 discussed the design and development phase of the Design Science Research Methodology (DSRM). The solution discussed in Chapter 4 was iteratively developed to produce usable prototypes. The next phase of the DSRM is the evaluation of the solution to rigorously demonstrate its utility, quality and efficacy. To fulfil this aim, a field study was conducted with twelve participants and one medical practice in Port Elizabeth over a period of two weeks. The results of the field study demonstrate and validate the design decisions made in the development of the prototype applications. The communication phase of the DSRM is also addressed in this chapter.

The results of the study were analysed to extract design recommendations for developing similar solutions. The evaluation objectives and metrics are discussed in Section 5.3. The results of the field study are presented in Section 5.4. Section 5.5 discusses the design implications of the field study. Section 5.6 presents the conclusions of the field study.

5.2 Evaluation Design

Dansky *et al.*, (2006) present a framework for evaluating eHealth Research. Their framework identifies four dimensions of eHealth evaluation namely:

- (i) Design and methodology: The design should be rigorous, have an adequate sample size and follow analytical procedures that conform to statistical validity requirements.
- (ii) Technological challenges: The technology should be tested prior to an evaluation. This ensures a smooth evaluation process.
- (iii) Ethical considerations: Ethics approval should be obtained prior to carrying out eHealth evaluation studies.

- (iv) Logistic or administrative factors: The availability and support of medical staff should be considered when planning an evaluation study.

The first dimension (design and methodology issues) was addressed through this research study by following the DSRM as explained in Chapter 1. The second dimension (challenges relating to technology) was addressed in Chapter 3, where a review of existing mobile health systems and architectures for ubiquitous access to health information was conducted. For example, mobile-centred PHR systems were preferred over smart card centred PHR systems because mobile devices are more widely used than smart cards in South Africa.

The third dimension (ethical considerations) was addressed by obtaining ethical clearance from the NMMU REC-H, and obtaining permission from the NMMU Health Services department to carry out this study on their premises.

The fourth dimension (logistic or administrative factors) was addressed by partnering with the NMMU Health Services department, who volunteered staff.

5.2.1 Evaluation Objectives

The aim of the field study was to evaluate the usability and performance of both the mobile and web applications in a real work context. This helped to achieve the secondary objective of the research by identifying usability problems and providing recommendations for future work. The self-reported data from the questionnaires provided information about the participants' perceptions of the PHR system.

5.2.2 Participants

The participants were categorised into two types:

- (i) Patient Participants.
- (ii) Medical Practice Administrator.

Patient participants were essential in evaluating the mobile application and the web application. These participants installed the mobile application on their phones. The patient participants also helped to evaluate the functionality of the web application by visiting NMMU Health Services to

carry out scheduled medical examinations. Patient participants only interacted with the mobile application.

The medical practice administrator (NMMU Health Services) was essential in evaluating the web application. The medical practice administrator was given access to a cloud-hosted web application. NMMU Health Services made their medical personnel available for the study for a period of two weeks.

Table 5-1 shows the Android experience of the patient participants. All the participants had their own Android phones. Android experience was important for the field study since one of the prototypes was an Android application. This ensured that participants were comfortable with Android design patterns.

Table 5-1: Participant experience with Android phones (n=12)

Experience with Android Phones	
Time	Number of Participants
0-6 Months	5
1-2 Years	4
> 2 Years	3

Table 5-2 shows the gender of the participants. Ten of the twelve participants were male while two were female. All patient participants were between 18 and 29 years of age.

Table 5-2: Gender of Participants (n=12)

Gender	
Male	10
Female	2

The mobile application was installed on each of the participant's phones. The mobile application logged the following data:

- (i) Time taken on each task.
- (ii) The CP-ABE: key generation and encryption times.

On completion of the tasks, the mobile application automatically emailed the log files to the principal researcher for analysis.

The patient participants were required to identify themselves to the medical practice administrator as being part of the “PHR Research Study”. Once the patient participants identified themselves, the medical practice administrator searched for their names on the web application and provided them with a set of medical examinations to choose from. The medical practice administrator uploaded each patient’s medical results onto the web application. The patients were then able to view their medical results on their mobile phones.

A follow up visit was arranged for each patient. The medical practice administrator was tasked with updating their health records. The web application logged the decryption time of the medical record identifiers. The patient participants and medical practice administrator then filled out questionnaires for evaluation purposes. The results of the field study are presented in Section 5.4.

5.3 Field Study Design

For the mobile application, a poster inviting participants was displayed in the NMMU Computing Sciences Department. Twelve participants volunteered to participate in the evaluation. The goal of the study was explained to each participant, and the degree of time required for participation was discussed. Each participant signed a consent form before participating.

The medical practice administrator evaluated the web application. Performance and self-reported metrics were captured during the field study to evaluate the interaction and usability of the prototype applications.

Each of the twelve patient participants was required to install the mobile application on their own phones and complete tasks specified later in Section 5.3.4. The participants were also required to make two visits to the NMMU Health Services and undergo voluntary medical examinations as determined by the medical practice administrator. The results of each patient’s medical examinations were uploaded to the web application by the medical practice administrator at NMMU Health Services. The participants were then able to view their results on their mobile devices. A figure illustrating this interaction is presented in Appendix M.

The participants completed post-test and post-study questionnaires. The questions on the questionnaires were based on the evaluation goals, which mainly focused on measuring self-reported metrics.

5.3.1 Evaluation Metrics

Usability metrics are a way of measuring or evaluating a particular object. They are observable and quantifiable (Tullis & Albert, 2008c).

Metrics for evaluating the utility of the prototype applications are categorised into two categories:

a. Self-Reported Metrics

Self-Reported data provides information about the participants' perceptions of the system after interacting with it. The metrics serve to measure the following properties:

- (i) Ease of use: How easy was it for the participants to complete the tasks
- (ii) User satisfaction: How satisfied the participants were with the system

b. Performance Metrics

Task success and time on task were chosen because they are easy to measure in a field study. Error rate was not measured as it was difficult to accurately measure in the context of a field study.

- (i) Task success: measures whether the participants were able to complete the tasks as assigned. Task success can either be measured as a binary value (completed/not-completed) or assigned different levels of success (Tullis & Albert, 2008a). This study measured level of success.
- (ii) Time on task: measures how much time is expected to complete a given task.

5.3.2 Evaluation Instruments

Participants were provided with a task list (Appendix E). Effectiveness was determined based on the extent to which participants were able to complete the tasks provided. The successful completion of the tasks was reflected on the web application once the participants shared their data with NMMU Health Services. This was used to determine the task success rate.

Patient participants completed an After Scenario Questionnaire (ASQ) for each of the tasks. This was done in order to provide insight into the perceived efficiency, effectiveness and satisfaction of each task (Tullis & Albert, 2008b).

Post-test questionnaires were administered at the end of the evaluation, with different questionnaires for the patient participants and the medical practice administrator. The aim was to capture the participants' and medical practice administrators' overall perception of the system.

User Tasks

The Norman Nielsen Group (2014) maintain that good usability tasks should:

- (i) Be realistic: The tasks should emulate the real world usage of the system.
- (ii) Actionable: Tasks should have a clear end goal.
- (iii) Avoid clues and describing steps: Tasks should not give away clues to the participants.

These guidelines were applied in developing the tasks of the study. The tasks were grouped into two categories:

- (i) **Patient Participants**

Each participant was provided with nine tasks (Appendix E). The participants were required to complete the tasks before visiting the medical service provider. The tasks covered the main functionality of the system.

- (ii) **Medical Practice Administrator**

NMMU health services made their medical staff available for the field study during off peak hours (2-5pm).

5.4 Field Study Evaluation Results

The analysis of the results from the field study is presented in this section. The results are presented in two different sections. Section 5.4.1 discusses the performance results while Section 5.4.2 discusses the user satisfaction results.

5.4.1 Performance Results

Task Success

Each task was designed to have a clear completion state. This enabled task success to be measured.

Two sets of tasks were used:

- (i) Patient tasks: A task was considered successful if data entered by patients using mobile phones was submitted to the cloud service.
- (ii) Medical tasks: Medical tasks were considered successful if the medical practice administrator could successfully access and update a patient's consultation notes using the web application.

Patient Task Success

Patient tasks were assigned different levels of success as shown below:

- (i) **Completed task:** 1.0
- (ii) **Partial success:** 0.5
- (iii) **No success:** 0.0

The distinction between no success and partial success could not be automatically determined. Hence, it was necessary to interview participants afterwards to determine the extent of their partial success.

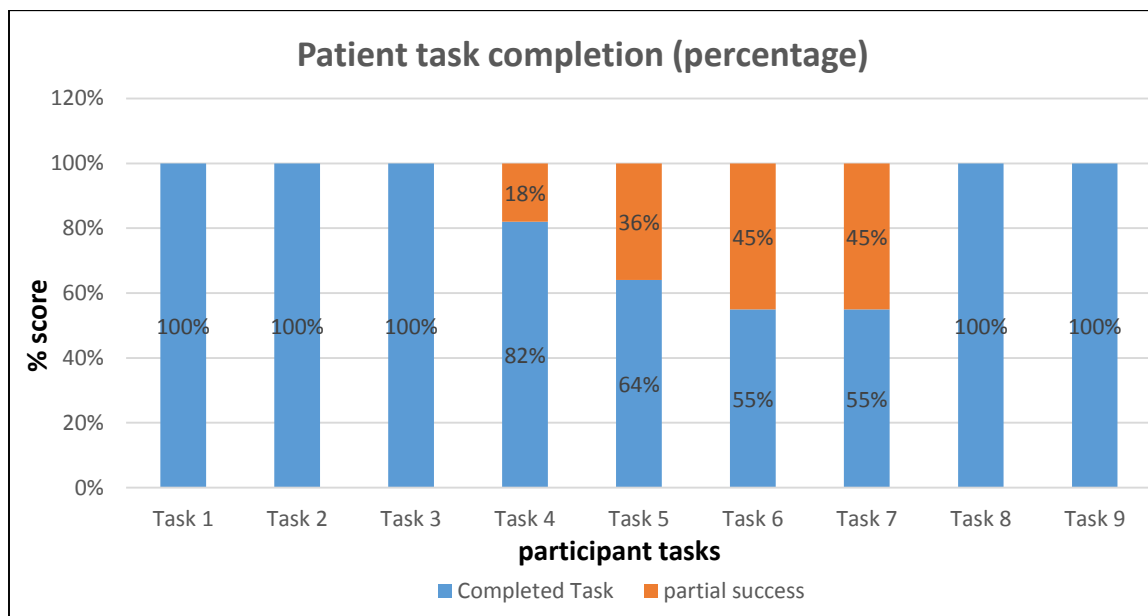


Figure 5-1: Patient Task Success (n=12)

The list of tasks is shown in Appendix E. Tasks 4-7 required the participants to enter their allergies, immunisations, conditions and medication data. Some of the participants informed the researcher that they did not have such information, hence they skipped these tasks.

Time on Task

The mobile application logged the time spent on each of the data entry tasks and also the time spent generating a patient's Public and Master Secret Keys. The encryption time of the medical ID and the Medical practice's Secret Key Generation time were also logged.

It was observed that the patient participants took varied amount of times/durations to complete the data entry tasks (Tasks 3-7). The times ranged from 30 seconds to 3 minutes. The participants were interviewed to find out why they took different times. Some of them explained that they had to search their bags to find their medical insurance information and this took up time while others said they were reading the fields carefully and thinking about what to enter. The time on task information is therefore not presented as it is not of real importance when dealing with medical information; accuracy is more important.

Each patient was associated with one Master and one Public key. These keys are used in the CP-ABE algorithm as discussed in Chapter 2 and illustrated in Chapter 4. The keys were generated when each participant registered an account using his or her mobile phone.

The Master key and Public key generation times varied from 1 to 4 seconds for the participants. The participants did not complain about the application being slow. This is because the keys were generated in a background thread, ensuring the user interface remained responsive.

The generation of private keys for the NMMU Health Services for various participants took a longer amount of time between 8 and 17 seconds. The generation of the private keys was done in a background thread and did not affect the usability of the mobile application. A private key is generated for each new medical practice that is added by a patient. A graph of the generation times is presented in Figure 5-2.

Bethencourt *et al.*, (2007) state that, the running time of the CP-ABE key generation and encryption algorithm is almost linear with respect to the number of leaf nodes in the access policy. The polynomial operations at internal nodes amount to a modest number of multiplications and do

not significantly contribute to the running time. Both remain feasible for even the largest problem instances.

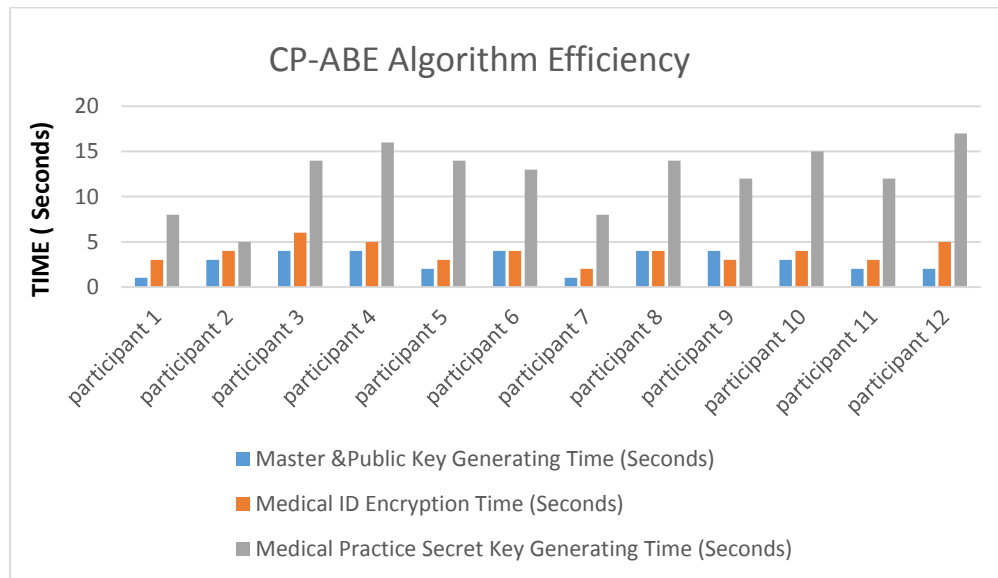


Figure 5-2: Encryption Performance (n=12)

The NMMU Health Services had a secret key (SK) for each patient, which together with a given patient's public key (PK) can be used to decrypt a patient's medical record identifier field. The medical record associated with the decrypted key could then be accessed by the medical practice as specified in the permissions algorithm.

5.4.2 User Satisfaction Results

A post-task questionnaire and a post-test questionnaire were used to capture the user satisfaction results (Appendix G and Appendix H). The post task questionnaire captured perceived ease of use, efficiency and satisfaction of the mobile and web applications. The post-test questionnaire captured the overall perceived usefulness, efficiency and satisfaction of the system. The post-test questionnaire also included an open-ended section to capture qualitative data.

5.4.2.1 Post Task Satisfaction Results

Each participant completed a questionnaire after each task. The post-test questionnaire was adapted from the After Scenario Questionnaire (ASQ) to evaluate each of the tasks. The questionnaire is attached in Appendix I. There were nine patient tasks. Five of the nine tasks were data entry tasks. The data entry tasks were evaluated as one task. Hence, the five post-test tasks were:

- (i) Registering to use the mobile application.
- (ii) Sharing health data with NMMU health services.
- (iii) Adding personal health information to the application.
- (iv) Syncing a patient's health data to a cloud server.
- (v) Viewing medical data uploaded by medical providers.

The results indicated that the patient participants were generally satisfied with the interaction with the different tasks as shown in Table 5-3.

Registering to use the mobile application and viewing medical consultation data uploaded by NMMU Health Services had the highest rating and received an overall median rating of 6.5/7.0 (Likert scale). The participants explained that the registration process was clear. The participants liked the ability to view their medical consultation data.

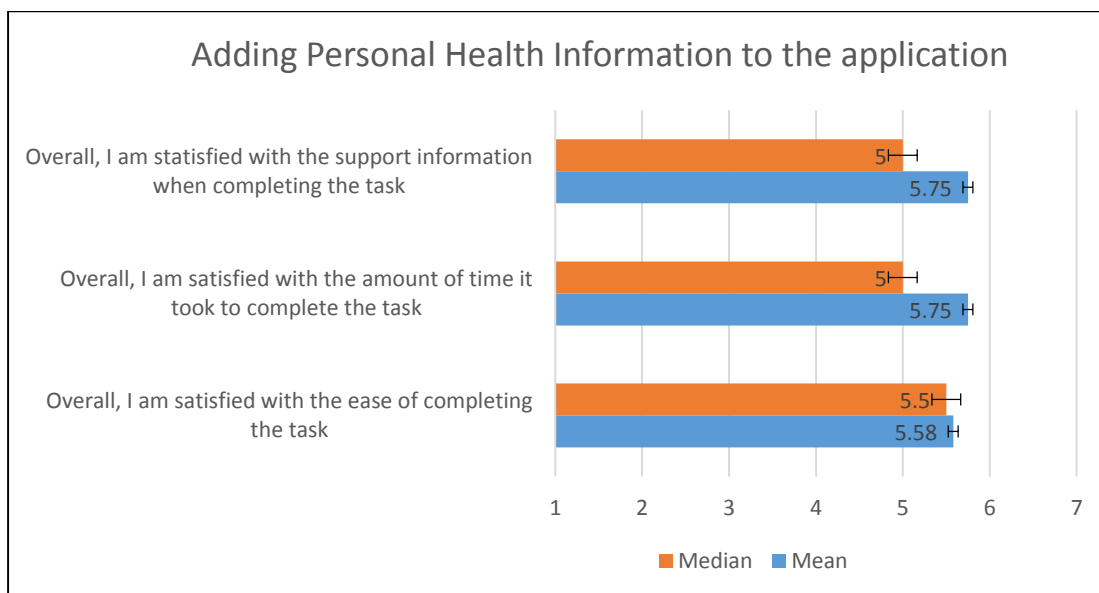
Adding personal health information to the mobile application received the lowest rating and a median value of 5.0/7.0 (Likert scale). The participants explained that they did not have all the information required, for example medication data, hence the poor ratings.

The ratings of the patient tasks are given in Table 5-3.

Table 5-3: Mean, Standard Deviation and Median rating of patient tasks (n=12)

Task	Mean (Max = 7.0)	Std. Deviation (Max = 7.0)	Median (Max = 7.0)
Registering to use the mobile application	6.33	0.97	6.5
Sharing health data with NMMU health services	6.33	0.72	5.5
Adding personal health information to the application	5.69	1.30	5.0
Syncing a patient's health data to a cloud server	5.94	1.43	5.5
Viewing medical consultation data uploaded by NMMU health services	6.47	0.51	6.5

Figure 5-3 illustrates the participant responses to adding personal health information.

**Figure 5-3: Adding health information to the mobile application (n=12)**

Five of the participants only had 0-6 months experience in Android, which could have affected their ratings.

The perceived usefulness of the mobile prototype had a mean score of 87.10%, which indicates that the participants thought that the prototype could be used to support ubiquitous management of PHRs. The satisfaction score was 90%. This indicates that the mobile application provided a highly positive user experience. The ease of use received a mean score of 91.40%.

The ease of learning received the lowest score of 85.70%. This can be attributed to the fact that participants always had to navigate back to the home screen in order to synchronise their data with the cloud server. A few participants assumed that the syncing was done automatically after they linked their accounts with the NMMU Health Services.

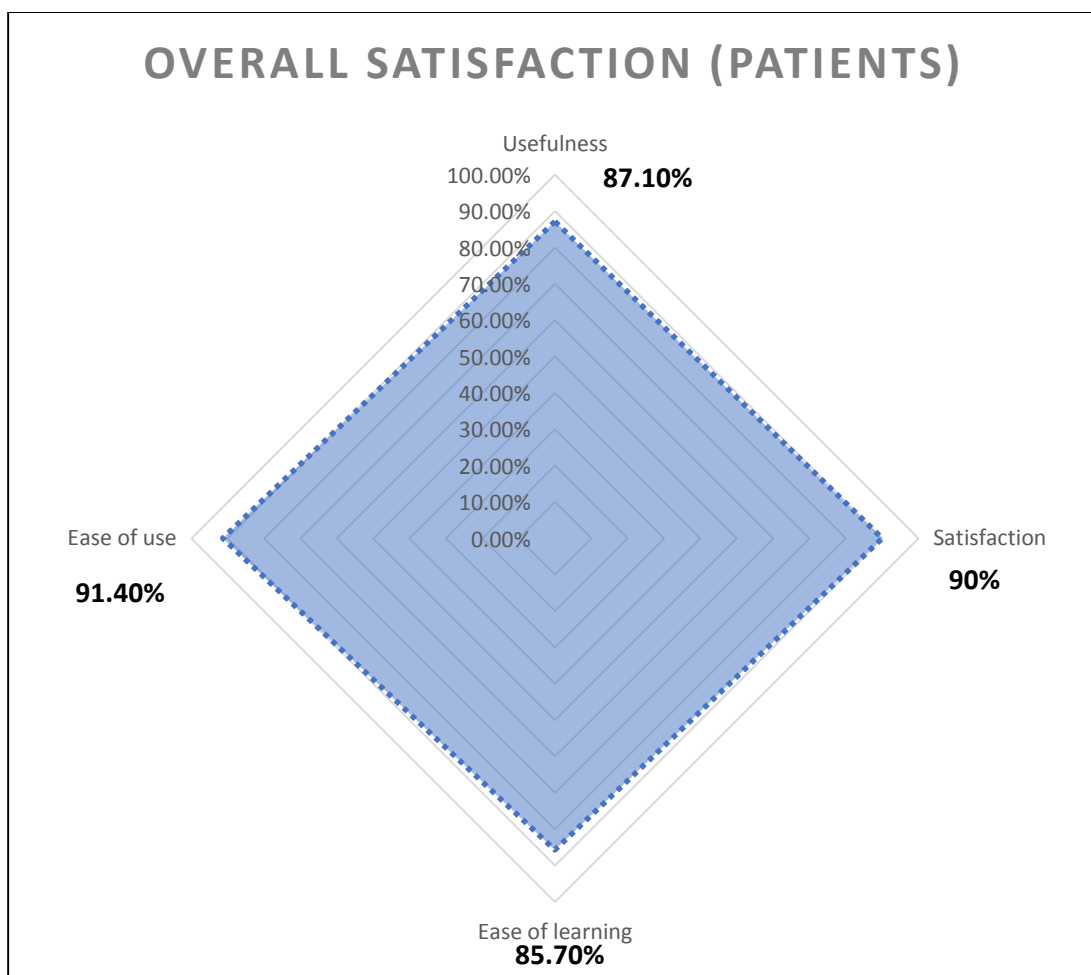


Figure 5-4: Ease of Use, Usefulness, Ease of Learning and Satisfaction (n=12)

The square shape of the radar chart in Figure 5-4 reflects the fact that the patient participants thought the mobile application was easy to use, easy to learn, useful and were generally satisfied with the system.

NMMU Health Services

Overall, the medical practice administrator found the system to be simple, easy to use and learn. Figure 5-5 illustrates the overall satisfaction of the medical practice administrator.

The medical practice administrator gave the system an overall satisfaction score of 5 out of 7 (Likert scale). The medical practice complained that the patient list was not updated asynchronously. That is, they had to re-login to view recently registered patients. The medical practice administrator also recommended that the patient list should be displayed in an alphabetical order. During the evaluation study, the patient list was sorted by order of patient registration.

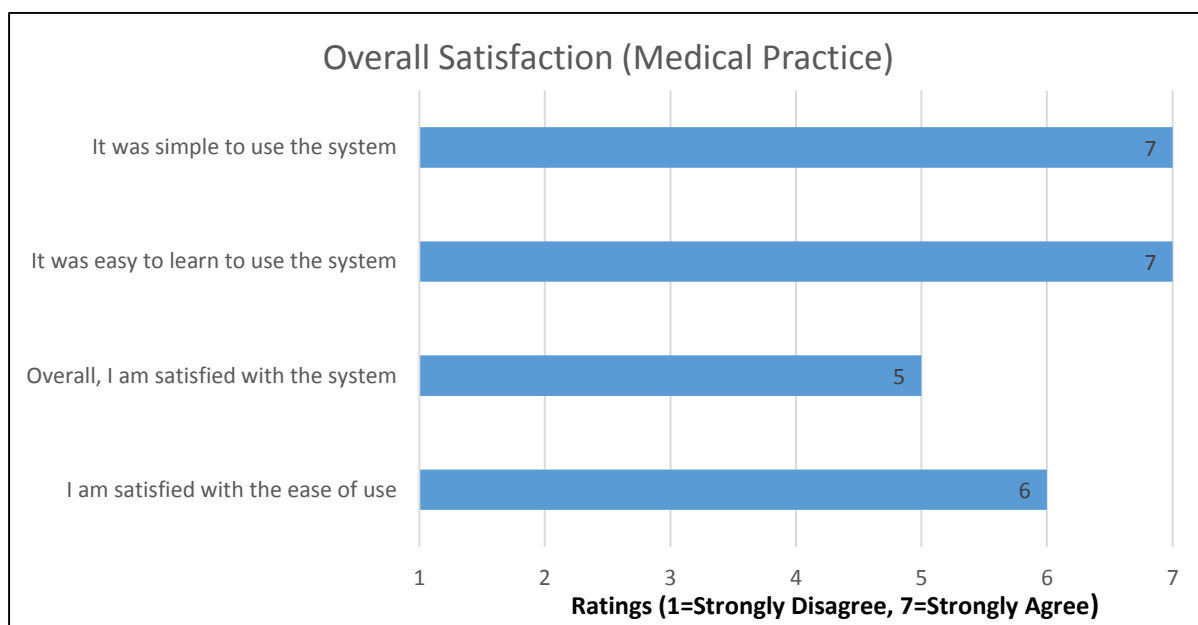


Figure 5-5: Overall Satisfaction (NMMU Health Services)

The medical practice administrator attributed the high scores of 7 and 6 to the fact that the system was simple to use and relevant to the day-to-day activities of the NMMU Health Services.

Searching for patients on the system

The low rating of (5.0/7.0) was attributed to the fact that the NMMU Health Services patient list was not sorted alphabetically.

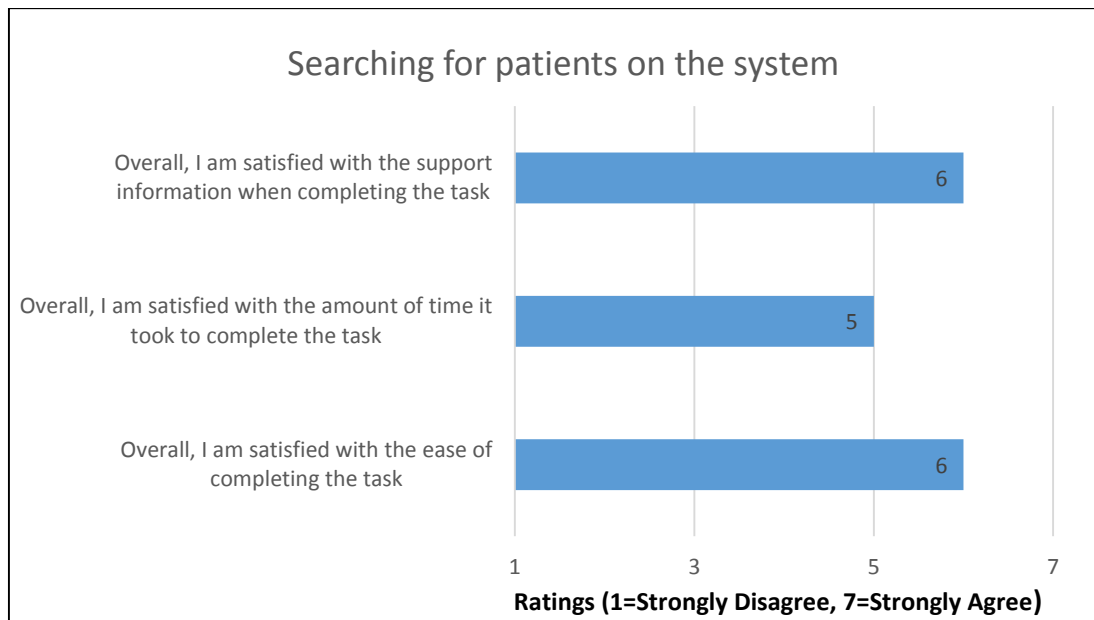


Figure 5-6: Searching for patients on the system

Viewing a patient's self-reported data

The medical practice administrator gave the task of being able to view a patient's self-reported data a perfect score of 7.0/7.0. This task is at the core of this research study; that is enabling ubiquitous access to a patient's medical information. A patient's medical record was organised in three distinct colour coded tabs as described below:

- (i) **Patient Generated Data:** A patient's self-reported data was displayed in the first tab. This information was displayed in tables.
- (ii) **Doctor Consultation Data:** A patient's medical history as captured by the medical practice administrator was displayed in the second tab. This layout made it easy for the medical practice administrator to view a patient's consultation data and also add new consultation notes
- (iii) **Medical Image Data:** The third tab consisted of a patient's image data such as x-rays

The NMMU medical practice administrator liked this layout design as illustrated in Figure 5-7.

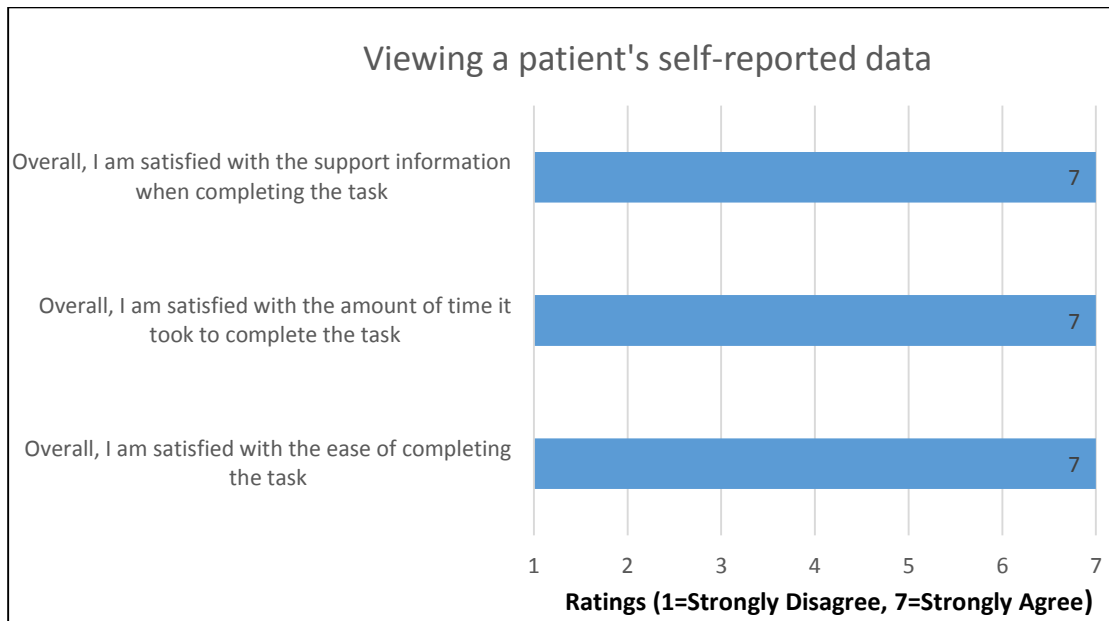


Figure 5-7: Viewing a patient's self-reported data

Adding a patient's consultation data

The medical practice administrator was generally satisfied with the functionality of adding a patient's consultation data (Figure 5-8). The medical practice administrator suggested that we add ICD9 (CDC, 2009) diagnosis codes to the consultation data entry form. This explains the low score of 5.0/7.0 (Likert scale) associated with the overall satisfaction of this task.

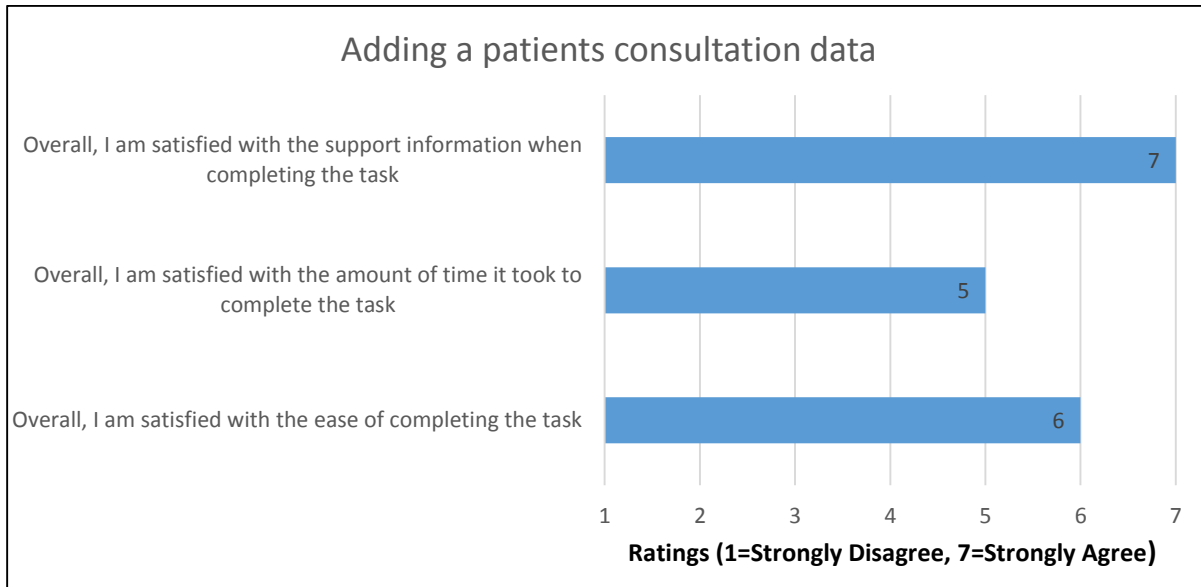


Figure 5-8: Adding a patient's consultation data (NMMU Health Services)

5.4.2.1 Qualitative Feedback Results

Qualitative data was captured from open-ended questions in the post-test questionnaire and comments from participants during the field study. The feedback for both patient participants and the medical practice administrator was categorised into positive, negative and general feedback. The feedback was categorised into two categories namely patient participant feedback (Table 5-4) and medical practice feedback (Table 5-5).

Patient Participants

Table 5-4: Feedback from patient participants

Positive Feedback	Frequency
Good to know and review medical information	6
The system is easy to use	5
I can effectively find medical practices	2
Registering was quick and easy- always a great start to an app	2
Negative Feedback	
Maybe add a label to show where the cloud back up button is	3
General Comments for Improvements	

Add a feature that reminds a person to revisit the health provider if the results were not as expected.	1
---	----------

The patient participants liked the feature that enabled them to know and review their medical consultation data (n=6). This supports the design decision to give patients read-only access to their medical consultation data. Participants thought that the application was easy to use (n=5). This supports the selection of participants with Android experience as illustrated in Section 5.3.3, since they were already familiar with the Android design patterns, which were used in the application. The ability to share medical information with different medical practices was one of the goals of this study. Two participants identified this feature as the most positive. Three participants identified the lack of an automatic back-up feature as the most negative aspect of the system. The prototype required participants to press a cloud backup icon. One participant noted that a feature that reminds patients of their upcoming medical visits would be nice.

NMMU Health Services

Table 5-5: Feedback from NMMU Health Services

Positive Feedback	Theme
“The patient is able to register himself before attending the clinic and their full records will be available if they go to another medical practice. I think this is a great system. The idea is fantastic. It maybe just needs a few tweaks”.	Functionality
Negative Feedback	Theme
“If someone registered while I was logged in, I had to logout and log in again to refresh the patient list. Patient list was generated in the order of registration instead of alphabetically”.	Efficiency
Suggestions	
(i) Include a Refresh button on the patient list	Efficiency

<p>(ii) Make it as quick and easy as possible for the medical practitioner to enter his notes. Medical practitioners do not have a lot of time between clients.</p> <p>(iii) Add medication drop boxes to speed up note taking.</p> <p>(iv) Consider adding medical diagnosis codes to speed up note taking. Board of Healthcare Funders of South Africa (BHF) can provide the WHO list.</p> <p>(v) The system can be expanded to include billing and pharmacies. If used in pharmacies and emergency medical facilities, it can potentially reduce prescription drug abuse.</p>	
--	--

The medical practice administrator liked the functionality that enabled patients to register themselves using their mobile phones and linking their accounts to a variety of medical practices. This functionality is directly related to Research Question 4 (RQ4), which is: *How usable and effective is the prototype in supporting PHR management?*

The medical practice administrator complained about the lack of a feature for automatically refreshing the patient list to show recently registered patients. This he said takes up valuable time. This limitation is addressed in Section 5.5. The medical practice administrator suggested an auto refresh button for the patient list. He also suggested integrating ICD9 diagnosis codes.

5.4.3 Discussion

The aim of the field study was to evaluate the interaction, usability and utility of the ubiquitous PHR management system by investigating the usefulness, ease of use and user satisfaction of both the mobile and web application prototypes. The field study also helped identify usability problems and recommendations for future work. The evaluation focused on real world interaction of patients and a medical practice. Self-reported and performance metrics were captured and analysed to meet the evaluation objectives.

The patient participants commented that the mobile prototype provided them with an easy way of sharing their health records with medical practice. The patient participants liked the simplicity of the mobile application.

Viewing medical notes shared by the medical practice received the highest mean rating. For example, some of the patient participants discussed ways to reduce their blood pressure after viewing the results on the mobile prototype. The patient participants were generally satisfied with the interaction and presentation of their medical health records.

The medical practice administrator was satisfied with the interaction and simplicity of the web application. The medical practice administrator, however, identified one major usability problem. The web application did not have an auto refresh when new patients registered while the medical personnel were logged into the system. The medical practice had to re-login to view the recently registered patients.

The medical practice administrator emphasised the importance and significance of such a system to the medical field in South Africa. The field study results thus provided insight into the interaction, usability and utility of the prototype applications, which were generally positive.

5.5 Design Implications

The following design recommendations were identified from the comments section of the post-test questionnaires:

Mobile Application

Backing up of information to a cloud server should be automatic after a user links up their profile with a medical practice. Three patient participants identified this as a problem. Currently a user has to explicitly back up their information. The application needs to be updated to allow automatic backup once a user makes a new entry. For optimal performance, the connectivity of the mobile phone should first be determined. Data should preferably be backed up when Wi-Fi is connected.

Web Application

- (i) The input of medical doctor notes should be made easier by providing medical diagnosis codes. The medical practice administrator at NMMU Health Services suggested that ICD-9 medical diagnosis codes should be incorporated into the web application. This will speed up consultation data entry.
- (ii) Auto refresh of the patient list should be implemented.

The web application should be made asynchronous so that a medical practice administrator who is logged on doesn't have to re-login to view recently added patients.

5.6 Conclusions

This chapter has addressed the evaluation phase of the Design Science Research Methodology (DSRM) explained in Section 1.7. The field study results of the mobile and web application prototypes developed in Chapter 4 were presented.

The evaluation focused on the real world usage of the system, that is, patients interacting with a medical care provider. Two categories of participants were involved namely:

Medical practice: Tasked with processing patient participants

Patients: Tasked with making visiting the NMMU Health Services and undergoing medical procedures.

Prior to the field study, ethical clearance was obtained from the university and special permission from the NMMU Health Services administration. This helped ensure the ethical legitimacy of the study.

Both categories of participants perceived the prototype applications as being useful, easy to learn and use. The patient participants identified the need to have automatic synchronisation of their data with all their connected medical practices. The medical practice administrator identified the need to have a medical practice's patient list updated asynchronously when they are logged in.

Ayana *et al.* (2001) note that PHRs do not necessarily improve patient health care. Some of the reasons for this is disinterest from patients and the medical care providers who have to input data into patient provided PHRs. This sentiment is true since the interview studies in Chapter 4 highlighted that medical care practitioners do not advocate for patients managing their health data.

The Hybrid Personal Health Record Management Model presented in Chapter 4 could thus be successfully implemented as a mobile and web-based application. The results of the field study show that the proposed model brings us closer to realising ubiquitous access to PHRs in South Africa. The next chapter concludes the research.

Chapter 6: Conclusion

6.1 Introduction

This chapter completes the last phase (communication) of the Design Science Research Methodology (DSRM) by discussing the contributions of this research study and recommendations for future work. The main objective of this research was:

Developing a model to facilitate ubiquitous access and secure sharing of PHRs in South Africa.

A model was developed using knowledge acquired from the existing literature and interview studies carried out with three medical practices in Port Elizabeth. This chapter revisits the objectives of this research to determine whether these objectives were achieved.

6.2 Achievements of Research Objectives

This research has shown that a ubiquitous Personal Health Record management system can be developed using the model presented in Chapter 4. The implementation of the developed model can be used to support ubiquitous access to PHRs in South Africa.

The sub-objectives that helped achieve the main objective were:

- (i) To identify the requirements for ubiquitous management of PHRs and existing user concerns that may hinder PHR adoption (Chapter 2).
- (ii) To review existing mobile health (mHealth) systems and architectures that can be used to support ubiquitous access and secure sharing of PHRs (Chapter 3).
- (iii) To design a model to facilitate ubiquitous access and secure sharing of PHRs and implement a system to validate the proposed model (Chapter 4).
- (iv) To evaluate the effectiveness and usefulness of the prototypes (Chapter 5).

Chapters 1 and 2 addressed Research Objective 1, which is concerned with problem identification. It was found that there is a lack of ubiquitous access to health records in South Africa. PHR data encoding standards were reviewed and the Personal Health Record System Standard (PHR-S) by the Clinical Document Architecture (CDA) was found to be the most applicable to South Africa.

The PHR system requirements were contextualised for this study by interviewing three local medical practices.

Research Objective 2 was answered in Chapter 3. Chapter 3 reviewed existing mHealth applications and architectures that can facilitate ubiquitous access to health information. It was observed that most of the applications support the PHR data elements. However, features to ensure the confidentiality of the data and enhance the usability of PHR applications needed to be improved. The hybrid PHR architecture was found to be the most suitable for use in South Africa.

Research Objective 3 was answered in Chapter 4. A Hybrid PHR Management Model was designed in Chapter 4 using the requirements obtained from Chapter 2 and the selected architecture from Chapter 3. A mobile and a web application prototype were implemented as proof of concept of the proposed model.

Research Objective 4 was answered in Chapter 5. A field study was carried out with one medical practice administrator from the NMMU Health Services and patient participants. The PHR management system was well received by both categories of participants.

6.3 Reflections on the HNSF

The National Health Normative Standards Framework for Interoperability in eHealth in South Africa (HNSF) was published in March 2014 by the South African National Department of Health (NDoH) and the Council for Scientific and Industrial Research (CSIR) (NDoH & CSIR, 2014).

The definitions of EMR, EHR AND PHR that are used in this research adhere to the definitions specified in the HNSF. A study of existing healthcare settings found the following on the maturity of Health Information Systems (HIS) in South Africa (NDoH & CSIR, 2014):

- (i) Almost all the clinics visited during a survey depended on only paper-based patient medical records.
- (ii) The vast majority of hospitals visited that supported HIS used the systems for admission and discharge. The patient demographics are printed out by medical clerks and included in a paper file. Patient information is not shared with any other medical facility.

The report on the maturity of current HIS by the HNSF further highlights the importance of this study.

6.4 Research Contributions

Several research contributions were made due to the successful completion of the research objectives as discussed in the previous section. These contributions are categorised into two namely: theoretical and practical. The theoretical contributions apply directly to systems in support of ubiquitous management of personal health information in South Africa. The practical contributions resulting from the research are applicable to the mHealth domain.

6.4.1 Theoretical Contributions

One of the goals of this research was to solve the problem of fragmented medical health information in South Africa. Literature was reviewed and interview studies were carried out with three medical providers with regard to the management of personal health information. The literature and interview studies were analysed to produce the requirements for ubiquitous management of personal health information in South Africa. The requirements produced represent a theoretical contribution. The requirements are:

Functional

A select set of functions from the PHR systems standard were chosen as discussed in Section 2.5. The selected functions are essential in enabling ubiquitous access and secure management of PHRs. The field study also identified the need to integrate medical diagnosis codes (ICD-9/10) into the web application. This can speed up the data entry process for medical practice administrators and also enable easy interpretation of consultation notes shared by medical practices.

Eight criteria, which can be used to evaluate PHR applications, are presented in Section 3.6. These criteria can be used by future PHR researchers and developers.

Data

The PHR data elements were contextualised for South Africa. Interview studies were carried out with three medical care providers with the aim of contextualising the PHR data elements discussed

in Section 2.6. A UML class diagram for the PHR system was discussed in Section 4.4. The UML class diagram can be used by other researchers.

Security and privacy

This research has identified the CP-ABE as the most suitable for securing PHRs in a cloud environment. This research affirms the view expressed in literature that personal information should be stored separately from medical information. Using the findings from literature reviews and interview studies, a Hybrid Personal Health Record Management model was designed. The model provides the following benefits:

- (i) Relevant data model for South Africa.
- (ii) Contextual customisation that enables medical providers to make use of both desktop computers and mobile devices to view patient information.
- (iii) Privacy preserving medical records sharing: Individuals can selectively grant access and revoke access rights to medical practices. The medical records are also encrypted when stored on third party servers.

The feedback provided by both the medical practice administrator and student participants during the evaluation study is valuable as it can be used in the development of future PHR systems.

6.4.2 Practical Contributions

One of goals of Design Science Research is the development of artefacts to solve a real world problem. Two prototype applications were developed as discussed in Section 4.5. An Android mobile application was developed for patients and a web-based application for medical practices. The prototype applications and the field study results can be used as a starting point for future research work.

6.5 Limitations

A number of limitations were encountered during the research. The first limitation was not finding more than one medical practice to participate in the field study. Due to this the patient participants only visited one medical practice. However, this limitation did not really impact the main objective of this study as both the medical practice participant and patient participants had a clear

understanding of how the system can be used by various medical providers. The model does not address the issue of efficient user revocation and key refreshing.

6.6 Future Research

A number of recommendations for future research were identified. The Hybrid PHR management model uses a hybrid centralised cloud storage service for the health information. This model can be adapted to support distributed cloud storage. This could be useful for medical practices, which may have reservations about centralised cloud storage.

The mobile application can be enhanced with sensors. That is, the mobile prototype could capture a patient's fitness data from wearable devices such as the Nike fuel band. This data can be collected and stored together with a patient's self-reported health data. The collected fitness data and a patient's health record can then be combined to identify any interesting health related patterns.

Future mHealth software developers should consider tailoring Open Source software to meet a specific need. For example, an Open Source implementation of the interoperability standards defined in the National Health Normative Standards Framework for Interoperability in eHealth in South Africa has been designed by Jembi Health Systems (Jembi, 2014). CommCare HQ is a US-based organisation that provides Open Source eHealth software that can be used as a building block for custom eHealth projects (CommCare, 2012).

It may be worthwhile to conduct a more extensive field study with multiple medical practices and patients. The knowledge gained from an extensive field study can further improve the Hybrid PHR Management model presented in Chapter 4.

References

- ABC. (2011, July 11). Smartcards to give patients records control. Retrieved October 9, 2013, from <http://www.abc.net.au/news/2011-07-12/smartcards-to-give-patients-records-control/2791252>
- Abdelsalam, H., & Hammer, J. (2004). UbiData: Requirements and Architecture for Ubiquitous Data Access. *ACM*, 33(4), 71–76. doi:10.1145/1041410.1041423
- Agrawal, R., Ailamaki, A., & Philip, A. (2008). The Claremont Report on Database Research. *ACM SIGMOD Record*, 37(3), 9–19. doi:10.1145/1462571.1462573
- AHIMA. (2013). myPHR. Retrieved July 11, 2013, from <http://myphr.com/>
- Alhaqbani, B., & Fidge, C. (2008). Access Control Requirements for Processing Electronic Health Records, 371–382. Retrieved from http://link.springer.com/chapter/10.1007%2F978-3-540-78238-4_38
- Android Team. (2012). Syncing to the Cloud | Android Developers. Retrieved September 30, 2013, from <http://developer.android.com/training/cloudsync/index.html>
- Angst, C., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339–370. Retrieved from <http://dl.acm.org/citation.cfm?id=2017430>
- Apache. (2005). Apache CouchDB. Retrieved September 29, 2013, from <http://couchdb.apache.org/>
- Appy Awards. (2013). Appy Awards. Retrieved June 4, 2013, from <http://appyawards.net/#>
- Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1), 1–54. doi:10.1145/2379776.2379779
- Ayana, M., Pound, P., Lampe, F., & Ebrahim, S. (2001). Improving stroke patients' care: a patient held record is not enough. *BMC Health Services Research*, 1, 1. doi:10.1186/1472-6963-1-1
- Bakker, a R. (2006). The need to know the history of the use of digital patient data, in particular the EHR. *International Journal of Medical Informatics*, 76(5-6), 438–41. doi:10.1016/j.ijmedinf.2006.09.009
- Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient Controlled Encryption : Ensuring Privacy of Electronic Medical Records. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 103–114). New York. doi:10.1145/1655008.1655024

- Bertini, E., Gabrielli, S., & Kimani, S. (2006). Appropriating and assessing heuristics for mobile computing. In *Advanced Visual Interfaces* (pp. 119–126). New York. doi:10.1145/1133265.1133291
- Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)* (pp. 321–334). Berkeley, CA: IEEE. doi:10.1109/SP.2007.11
- Blue Cross. (2013). Your personal health record. Retrieved August 27, 2013, from <http://www.bcbs.com/healthcare-partners/personal-health-records/PHR-ConsumerBrochure.pdf>
- Caligtan, C. a, & Dykes, P. C. (2011). Electronic health records and personal health records. *Seminars in Oncology Nursing*, 27(3), 218–28. doi:10.1016/j.soncn.2011.04.007
- CDC. (2009). International Classification of Diseases, Ninth Revision (ICD-9). Retrieved from <http://www.cdc.gov/nchs/icd/icd9.htm>
- Chaplin, S. (2007). The Health eCard: the way ahead for medical records? *Prescriber: The Journal of Prescribing Medicines Management*, 18(19), 28–29. doi:10.1002/psb.134
- Chun, W. (2012). What is Cloud Computing? Retrieved from <https://developers.google.com/appengine/training/intro/whatiscc>
- Clarke, J. L., Meiris, D. C., & Nash, D. B. (2006). Electronic personal health records come of age. *American Journal of Medical Quality : The Official Journal of the American College of Medical Quality*, 21(3 Suppl), 5S–15S. doi:10.1177/1062860606287642
- Coleman Alfred. (2010). *Developing An E-Health Framework Through Electronic Healthcare Readiness Assessment*. Nelson Mandela Metropiltan University. Retrieved from <http://dspace.nmmu.ac.za:8080/xmlui/handle/10948/1519>
- CommCare. (2012). Developer Resources. Retrieved from <http://www.commcarehq.org/support/#for-developers>
- Dansky, K. H., Thompson, D., & Sanner, T. (2006). A framework for evaluating eHealth research. *Evaluation and Program Planning*, 29(4), 397–404. doi:10.1016/j.evalprogplan.2006.08.009
- Dillon, A. (2002). Information architecture in JASIST: Just where did we come from? *Journal of the American Society for Information Science and Technology*, 53(10), 821–823. doi:10.1002/asi.10090
- Donald, M., Ritter, J., Spears, C., & Dyke, P. Van. (2008). *HL7 Personal Health Record System Functional Model*. Retrieved from http://www.hl7.org/implement/standards/product_brief.cfm?product_id=88

- Donald T, M. (2010). EHR & PHR System Functional Model (EHR-S FM & PHR-S FM) and Standard. Retrieved April 15, 2013, from [http://www.cgallego.es/resources/EHR+\\$26+PHR+System+FM+EHIM+Barcelona+mtg+\\$282010-03-15\\$29.pdf](http://www.cgallego.es/resources/EHR+$26+PHR+System+FM+EHIM+Barcelona+mtg+$282010-03-15$29.pdf)
- Ed-informatics.org. (2012). EMR vs EHR vs PHR | ed-informatics.org. Retrieved May 27, 2013, from <http://ed-informatics.org/healthcare-it-in-a-nutshell-2/emr-vs-ehr-vs-phr/>
- EHR Work Group. (2008). Personal Health Record System Functional Model , Release 1 Draft Standard for Trial Use July 2008 Chapter Five : Information Infrastructure Functions. Retrieved March 17, 2014, from ftp://ftp.minsa.gob.pe/ODT/RNHCE/Recursos/Personal Health Record/PHR-FM_IN_R1_DSTU_DEC2008.pdf
- Ellis, T. J., & Levy, Y. (2010). A Guide for Novice Researchers : Design and Development Research Methods. In *Informing Science and IT Education Conference (InSite)* (pp. 107–118). Florida, USA: Informing Science Institute.
- Endsley, S., Kibbe, D. C., Linares, A., & Colorafi, K. (2006). An introduction to personal health records. *Family Practice Management*, 13(5), 57–62. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/16736906>
- EPDA. (2013). European Directory of Health Apps 2012-2013. Retrieved April 15, 2013, from http://www.hl7.org/documentcenter/public_temp_821D7E15-1C23-BA17-0C6265DFB732D988/wg/mobile/pv_appdirectory_final_web_300812.pdf
- Eysenbach, G. (2001). What is e-health? *Journal of Medical Internet Research*, 3(2), E20. doi:10.2196/jmir.3.2.e20
- 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*. doi:10.1016/j.jbi.2012.12.003
- Ferranti, J. M., Musser, R. C., Kawamoto, K., & Hammond, W. E. (2006). The clinical document architecture and the continuity of care record: a critical analysis. In *JAMIA: Journal of the American Medical Informatics Association* (Vol. 13, pp. 245–52). doi:10.1197/jamia.M1963
- Fong, E. N., & Goldfine, A. H. (1989). Information Management Directions: The Intergration Challenge. *ACM SIGMOD Record*, 18(4), 40–43. doi:10.1145/74120.74125
- Garets, D., & Davis, M. (2006). *Electronic Medical Records vs . Electronic Health Records: Yes, There Is a Difference* (pp. 1–14). Retrieved from https://www.himssanalytics.org/docs/WP_EMR_EHR.pdf
- Google. (2013). Google Health – Google. Retrieved May 2, 2013, from http://www.google.com/intl/en_us/health/about/

- Gorp, P. Van, & Comuzzi, M. (2012). Addressing Health Information Privacy with a novel Cloud-Based PHR System Architecture. In *IEEE International Conference on Systems, Man, and Cybernetics* (pp. 1841–1846). Seoul: IEEE. doi:10.1109/ICSMC.2012.6378006
- HealthIT.gov. (2008). About the Personal Health Record (PHR) Model Privacy Notice | Policy Researchers & Implementers | HealthIT.gov. Retrieved July 12, 2013, from <http://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice>
- HealthIT.gov. (2013). What is the importance of a personal health record (PHR)? | FAQs | Providers & Professionals | HealthIT.gov. Retrieved May 27, 2013, from <http://www.healthit.gov/providers-professionals/faqs/what-are-benefits-personal-health-records>
- HealthSpek. (2013). PHR - Personal Health Record for iPad on the iTunes App Store. Retrieved June 4, 2013, from <https://itunes.apple.com/us/app/healthspek-phr-personal-health/id576488481?mt=8>
- Helal, S., Hammer, J., Zhang, J., & Khushraj, a. (2001). A three-tier architecture for ubiquitous data access. *Proceedings ACS/IEEE International Conference on Computer Systems and Applications*, 177–180. doi:10.1109/AICCSA.2001.933971
- Herold, R. (2002). What Is The Difference Between Security and Privacy? Retrieved March 11, 2013, from [http://www.informationshield.com/papers/Privacy and Security - Herold.pdf](http://www.informationshield.com/papers/Privacy%20and%20Security%20-%20Herold.pdf)
- Hevner, B. A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly-Research Essay*, 28(1), 75–105.
- HL7. (2013). Health Level Seven International - Homepage. Retrieved March 19, 2013, from <http://www.hl7.org/index.cfm?ref=nav>
- Hofstee, E. (2011). *Constructing a Good Dissertation*. (A. Denniston, Ed.) (p. 113). Johannesburg, South Africa: EPE NBC Building, Second Floor, C Block 113 Katherine Street Sandton South Africa.
- HPCSA. (2008). Health professions council of south africa: Guidelines on the Keeping of Patient Records. PRETORIA. Retrieved from http://www.hpcsa.co.za/Uploads/editor/UserFiles/downloads/conduct_ethics/rules/generic_ethical_rules/booklet_14_keeping_of_patience_records.pdf
- Huang, E., Tseng, T., Chang, M., & Taipei, N. (2010). Standardized Clinical Documents for Medical Information Exchanges. In *IT Professional* (Vol. 12, pp. 26–32). IEEE. doi:10.1109/MITP.2010.56
- IA. (2013). WHAT IS INFORMATION ARCHITECTURE? Retrieved August 4, 2013, from http://www.iainstitute.org/documents/learn/What_is_IA.pdf

- Ihs.gov. (1996). IHS HIPAA Security Checklist HIPAA SECURITY. Retrieved July 10, 2013, from http://www.ihs.gov/hipaa/documents/ihs_hipaa_security_checklist.pdf
- ISO. (1947). ISO Standards - ISO. Retrieved July 10, 2013, from <http://www.iso.org/iso/home/standards.htm>
- ISO/TR20514. (2005). *Health informatics — Electronic health record — Definition, scope and context* (Vol. 2005, p. 20). Geneva.
- ISO17799. (1992). ISO 17799 Implementation Portal. Retrieved from <http://17799.denialinfo.com/>
- Jembi. (2014). ICT4H-2014 Hackathon. Retrieved from <https://jembiprojects.jira.com/wiki/display/ICT4H14/ICT4H-2014>
- Jing, H., Haihong, E., Jian, D., & Guan, L. (2011). Survey on NoSQL Database. In *Pervasive Computing and Applications (ICPCA)* (pp. 363–366). Port Elizabeth: IEEE. doi:10.1109/ICPCA.2011.6106531
- Kaelber, D., & Jha, A. (2008). A research agenda for personal health records (PHRs). *JAMIA: Journal of the American Medical Informatics Association*, 15(6), 729–736. doi:10.1197/jamia.M2547
- 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. doi: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), 171–181. doi:10.1197/jamia.M0978
- Klasnja, P., & Pratt, W. (2012). Healthcare in the pocket: mapping the space of mobile-phone health interventions. *Journal of Biomedical Informatics*, 45(1), 184–98. doi:10.1016/j.jbi.2011.08.017
- Koehler, N., Vujovic, O., & McMenamin, C. (2013). Healthcare professionals' use of mobile phones and the internet in clinical practice. *Journal of Mobile Technology in Medicine*. doi:10.7309/jmtm.2.1.2
- Kumar, S., Nilsen, W., Pavel, M., & Srivastava, M. (2013). Mobile Health :Revolutionizing Healthcare Through Trans- disciplinary Research. *IEEE Computer Society*, 46(1), 28–35. doi:10.1109/MC.2012.392
- Kwankam, S. Y. (2004). What e-Health can offer. *Bulletin of the World Health Organization*, 82(10), 800–2. Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2623036&tool=pmcentrez&rendertype=abstract>

- Kyazze, M., Wesson, J., & Naude, K. (2014). The design and implementation of a ubiquitous personal health record system for South Africa. In *Global Telehealth 2014* (pp. 29 – 41). Durban: IOS Press EBooks. doi:10.3233/978-1-61499-456-5-29
- Lerman, J. (2011, November). Data Points - What the Heck Are Document Databases? *MSDN Magazine*. Retrieved from <http://msdn.microsoft.com/en-us/magazine/hh547103.aspx>
- Loseit.com. (2013). Lose It! - Succeed at weight loss with Lose It! Retrieved September 26, 2013, from <http://www.loseit.com/>
- 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. doi:10.1016/j.ijmedinf.2009.11.005
- Mars, M., & Seebregts, C. (2008). Country Case Study for e-Health South Africa. 2013. Retrieved July 24, 2014, from <http://ehealth-connection.org/files/resources/County Case Study for eHealth South Africa.pdf>
- Masiza, M., Mostert-Phipps, N., & Pottas, D. (2013). Patient preferences regarding storage media for medical records. In *HISA*. Port Elizabeth. Retrieved from <http://goo.gl/FM6KLM>
- Mayosi, B. M., Mekwa, N. J., Blackburn, J., Coovadia, H., Friedman, I. B., & Jeenah, M. (2011). 2011 National Health Research Summit Report. Retrieved from http://www.ul.ac.za/application/downloads/National_Health_Research_Summit_Report-2011.pdf
- McClain, I., & Thompson, E. (2010). The use of cell phone technology provides teens more control and independence and healthcare cost savings in the management of chronic disease. *Perspectives in Health Information Management / AHIMA, American Health Information Management Association*, 7, 1g. Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2966358&tool=pmcentrez&rendertype=abstract>
- Mentz, J., Kotze, P., & Merwe, A. van der. (2012). A Comparison of Practitioner and Researcher Definitions of Enterprise Architecture using an Interpretation Method. In C. Moller & S. Chaudhry (Eds.), *Advances in Enterprise Information Systems II* (pp. 11–26). doi:10.1201/b12295-1
- MHWG. (2013). Mobile Health Work Group. Retrieved April 15, 2013, from <http://www.hl7.org/Special/committees/mobile/index.cfm>
- Microsoft. (2013). HealthVault: a platform for connected health information and innovation. Retrieved May 2, 2013, from <http://msdn.microsoft.com/en-us/healthvault/jj128027>
- Mohamed, A. H. H. M., Tawfik, H., Al-Jumeily, D., & Norton, L. (2011). MoHTAM: A Technology Acceptance Model for Mobile Health Applications. *2011 Developments in E-Systems Engineering*, 13–18. doi:10.1109/DeSE.2011.79

- MongoDB. (2009). Introduction to MongoDB. Retrieved September 17, 2013, from <http://www.mongodb.org/about/introduction/>
- MSHV. (2013). HealthVault. Retrieved May 2, 2013, from <https://www.healthvault.com/za/en>
- Mukandatsama, C., & Wesson, J. (2013). Designing a Mobile Pill Reminder for Elderly Users in South Africa. *Health Informatics South Africa (HISA) 2013 Conference*. Retrieved from <http://goo.gl/gPFhpG>
- Munis, P. (2012). Partner Webinar: Electronic Health Records (EHRs) and MongoDB - Advancing the Data Platform for the Future | MongoDB. Retrieved September 29, 2013, from <http://www.mongodb.com/presentations/partner-webinar-electronic-health-records-ehrs-and-mongodb-advancing-data-platform>
- Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2014). Personal Health Records: Design considerations for the South African context. In *DDR*. Cape Town, 8-10 September 2014. Retrieved from <http://hdl.handle.net/10204/7712>
- Myfitnesspal.com. (2013). myfitnesspal. Retrieved September 26, 2013, from http://www.myfitnesspal.com/welcome/learn_more
- Narayan, S., Gagné, M., & Safavi-Naini, R. (2010). Privacy preserving EHR system using attribute-based infrastructure. *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop - CCSW '10*, 47–52. doi:10.1145/1866835.1866845
- NDoH. (2012). eHealth Strategy South Africa 2012-2016. Retrieved from http://www.isftech.org/media/south_africa_national_ehealth_strategy_2012_2016
- NDoH, & CSIR. (2014). *National Health Normative Standards Framework for Interoperability in eHealth in South Africa* (pp. 32–35; 145–152). Retrieved from <http://hufee.meraka.org.za/Hufeesite/staff/the-hufee-group/paula-kotze-1/hnsf-complete-version>
- Nielsen Norman Group. (2014). Turn User Goals into Task Scenarios for Usability Testing. Retrieved September 15, 2014, from <http://www.nngroup.com/articles/task-scenarios-usability-testing/>
- OCR Hipaa, P. (2003). Standards for privacy of individually identifiable health information. *Health Care Law Monthly*, 502(d), 13–20. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/16381381>
- Offermann, P., & Platz, E. R. (2009). Outline of a Design Science Research Process. In *Desrist 2009 4th International Conference on Design Science Research in Information Systems and Technology*. doi:10.1145/1555619.1555629
- Open Clinical. (2011). e-Health. Retrieved June 20, 2013, from <http://www.openclinical.org/e-Health.html>

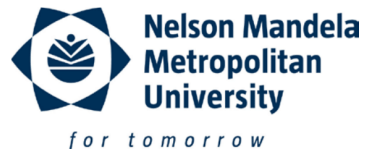
- OpenShift. (2014). OpenShift. Retrieved from <https://www.openshift.com/>
- Peffers, K., Gengler, C. E., Rossi, M., Hui, W., & Bragge, J. (2006). The Design Science Research Process : A Model for Producing and Presenting Information Systems Research. In *Proceedings of First International Conference on Design Science in Information Systems and Technology (DESRIST)* (pp. 83–106). Claremont, CA, USA.
- Rašković, D., Milenković, A., & Groen, P. C. De. (2008). From Telemedicine to Ubiquitous M-Health : The Evolution of E-Health Systems. *Biomedical Information Technology*, 479–496. doi:10.1016/B978-012373583-6.50026-8
- Rindfleisch, T. C. (1997). Privacy, Information Technology, and Health Care. *Communications of the ACM*, 40(8), 92–100. doi:10.1145/257874.257896
- Rishel, W. (2009). Simple Interop: the PHR. Retrieved July 10, 2013, from http://blogs.gartner.com/wes_rishel/2009/12/31/simple-interop-the-phr/
- Rizo, C., Enkin, M., Jadad, A., & Oh, H. (2005). What is eHealth (3): a systematic review of published definitions. *Journal of Medical Internet Research*, 7(1). doi:10.2196/jmir.7.1.e1
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (pp. 113;127;136–160).
- Simons, W., Mandl, K., & Kohane, I. (2005). The PING personally controlled electronic medical record system: technical architecture. *JAMIA: Journal of the American Medical Informatics Association*, 12(1), 47–54. doi:10.1197/jamia.M1592.
- SITA. (2010). The National Strategic Framework For EHR Implementation In South Africa. Retrieved April 11, 2013, from http://www.pnc.gov.za/images/stories/focus_area/report/ehr_fm.pdf
- Solomon, M. G., & Chapple, M. (2005). Introducing Computer and Network Security. In *Information Security Illuminated, 1st Edition* (pp. 2–5). Jones and Bartlett.
- Steele, R., & Lo, A. (2012). Personal Health Record Architectures : Technology Infrastructure Implications and Dependancies. *JASIST*, 63(6), 1079–1091. doi:10.1002/asi.22635
- Steele, R., & Min, K. (2010). HealthPass: Fine-Grained Access Control to Portable Personal Health Records. In *2010 24th IEEE International Conference on Advanced Information Networking and Applications* (pp. 1012–1019). IEEE. doi:10.1109/AINA.2010.176
- Stefan, E. (2013). NoSQL Your Ultimate Guide to the Non-Relational Universe! Retrieved from <http://nosql-database.org/>
- Steiert, H.-P. (1998). Towards a component-based n-Tier C/S-architecture. *Proceedings of the Third International Workshop on Software Architecture - ISAW '98*, 137–140. doi:10.1145/288408.288443

- Stonebraker, M., Abadi, D. J., Harizopoulos, S., & Helland, P. (2007). The End of an Architectural Era (It 's Time for a Complete Rewrite). In *VLDB '07 Proceedings of the 33rd international conference on Very large data bases* (pp. 1150–1160). Retrieved from <http://dl.acm.org/citation.cfm?id=1325981>
- Sumriddetchkajorn, S., Somboonkaew, A., & Chanhorm, S. (2012). Mobile device-based digital microscopy for education, healthcare, and agriculture. *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, 1–4. doi:10.1109/ECTICon.2012.6254186
- Sun, J., & Fang, Y. (2010). Cross-domain data sharing in distributed electronic health record systems. *IEEE Transactions on Parallel and Distributed Systems*, 21(6), 754–764. doi:10.1109/TPDS.2009.124
- Szolovits, P., Doyle, J., Long, W. J., & Kohane, I. (1994). Guardian Angel : Health Information Systems. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.27.2267>
- 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 : JAMIA*, 13(2), 121–6. doi:10.1197/jamia.M2025
- Tudorica, B. G., & Bucur, C. (2011). A comparison between several NoSQL databases with comments and notes. In *Roedunet International Conference (RoEduNet)* (pp. 1–5). Iasi: IEEE. doi:10.1109/RoEduNet.2011.5993686
- Tullis, T., & Albert, B. (2008a). Performance Metrics. In *Measuring the User Experience* (pp. 63–75).
- Tullis, T., & Albert, B. (2008b). Post-Task Ratings. In *Measuring the User Experience* (pp. 128–134).
- Tullis, T., & Albert, B. (2008c). What are usability metrics. In *Measuring the User Experience* (pp. 7–8).
- US DoH. (2006). *Personal Health Records and Personal Health Record Systems* (pp. 14–24;). Washington, D.C. Retrieved from <http://www.ncvhs.hhs.gov/0602nhirpt.pdf>
- US.DoH. (2007). *Consumer Empowerment : Consumer Access to Clinical Information Detailed Use Case*. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/government/bok1_036406.pdf
- Vital Wave Consulting. (2009). *mHealth for Development: The Opportunity of Mobile Technology for Healthcare in the Developing World. Foundation Partnership, 2009. Technology* (Vol. 46, pp. 1–70). Vital Wave Consulting. Retrieved from http://www.globalproblems-globalsolutions-files.org/unf_website/assets/publications/technology/mhealth/mHealth_for_Development_full.pdf

- WEDI. (2007). *Personal Health Records : An Industry Primer from the Privacy and Security Perspective Personal Health Records : An Industry Primer from the Privacy and Security* (Vol. 20191). Reston, Virginia.
- Yarbrough, A. K., & Smith, T. B. (2007). Technology acceptance among physicians: a new take on TAM. *Medical Care Research and Review*, *64*(6), 650–72.
doi:10.1177/1077558707305942
- Zhang, R., & Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. In *2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)* (pp. 268–275). Miami, FL: IEEE. doi:10.1109/CLOUD.2010.62
- Zimmermann, P. (1991). An Introduction to Cryptography (pp. 11–36). Network Associates, Inc. Retrieved from <ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf>

Appendices

Appendix A: Ethics Clearance Letter



• PO Box 77000 • Nelson Mandela Metropolitan University
• Port Elizabeth • 6031 • South Africa • www.nmmu.ac.za

Vice-Chairperson: Research Ethics Committee (Human)
Tel: +27 (0)41 504-2235

Ref: [H14-SCI-CSS-008/Approval]

Contact person: Mrs U Spies

20 August 2014

Prof J Wesson
Faculty of Science
Department: Computing Science
09-02-13
South Campus

Dear Prof Wesson

A MODEL FOR MANAGING PERSONAL HEALTH RECORDS USING MOBILE DEVICES IN SOUTH AFRICA

PRP: Prof J Wesson
PI: Mr M Kyazze

Your above-entitled application for ethics approval served at Research Ethics Committee (Human).

We take pleasure in informing you that the application was approved by the Committee.

The ethics clearance reference number is **H14-SCI-CSS-008** and is valid for three years. Please inform the REC-H, via your faculty representative, if any changes (particularly in the methodology) occur during this time. An annual affirmation to the effect that the protocols in use are still those for which approval was granted, will be required from you. You will be reminded timeously of this responsibility, and will receive the necessary documentation well in advance of any deadline.

We wish you well with the project. Please inform your co-investigators of the outcome, and convey our best wishes.

Yours sincerely

Prof CB Cilliers
Chairperson: Research Ethics Committee (Human)

cc: Department of Research Capacity Development
Faculty Officer: Science

Appendix B: HIPAA Technical safeguards

HIPAA Technical Safeguards		
Security Reference	Rule	Safeguard (R)= Required (A) = Addressable
164.312(a)(1)		Access Controls: Implement technical policies and procedures for eHealth information systems to allow access only to those persons or software programs that have been granted access rights
164.312(a)(2)(i)		Have you assigned a unique name and/or number for identifying and tracking user identity? (R)
164.312(a)(2)(ii)		Have you established and implemented procedures for obtaining necessary eHealth information during an emergency? (R)
164.312(a)(2)(iii)		Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)
164.312(a)(2)(iv)		Have you implemented a mechanism to encrypt and decrypt Personal health information (PHI)? (A)
164.312(b)		Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI? (R)
164.312(c)(1)		Integrity: Implement policies and procedures to protect PHI from improper alteration or destruction.
164.312(c)(2)		Implemented electronic mechanisms to ensure that PHI has not been altered or destroyed in an Unauthorised manner (A)
164.312(d)		Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access PHI is the one claimed? (R)
164.312(e)(1)		Ensure transmission security by implementing technical security measures to guard against Unauthorised access to PHI that is being transmitted.
164.312(e)(2)(i)		Have you implemented security measures to ensure that electronically transmitted PHI is not improperly modified without detection until disposed of? (A)
164.312(e)(2)(ii)		Have you implemented a mechanism to encrypt PHI whenever deemed appropriate? (A)

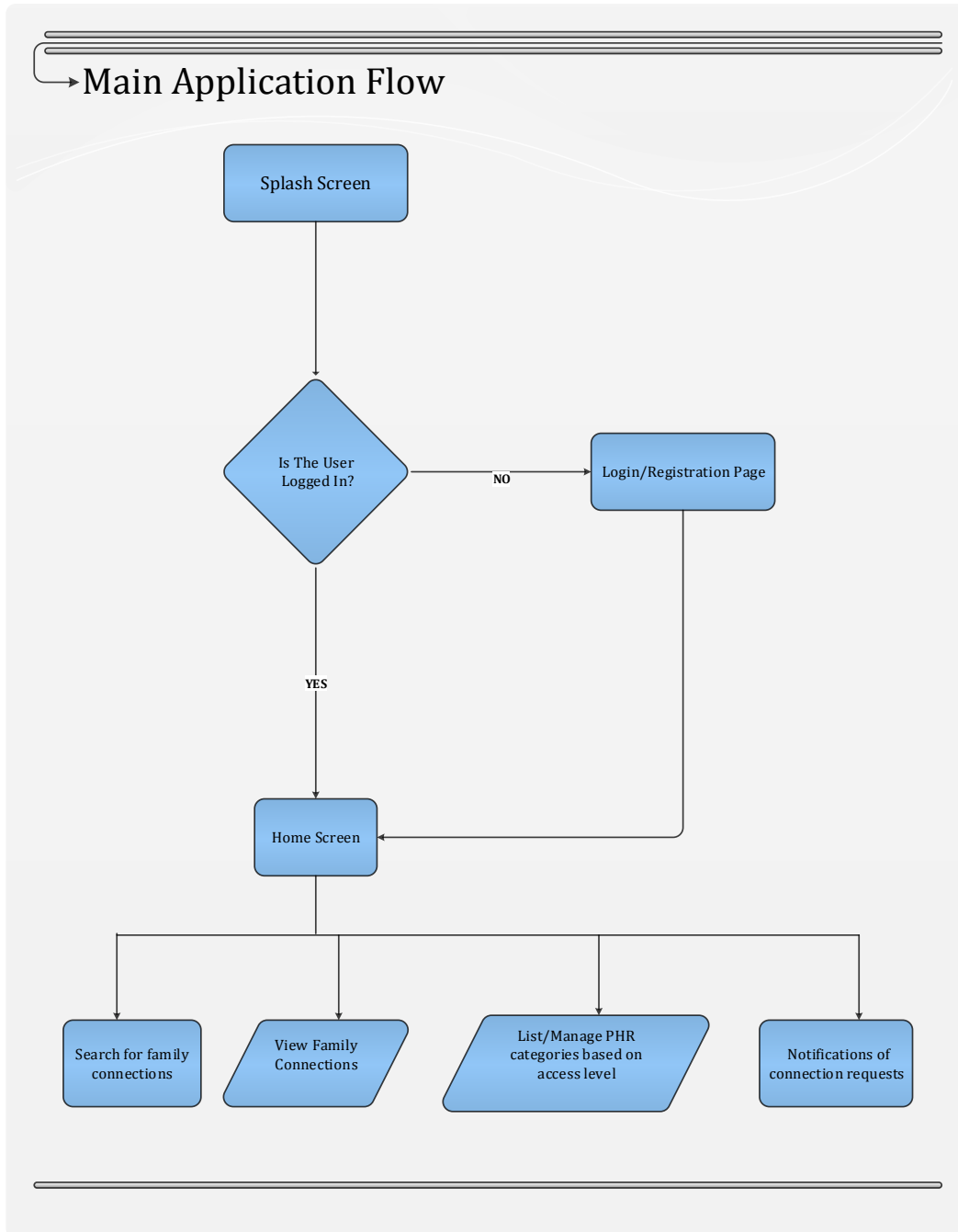
Appendix C: PHR Functional requirements

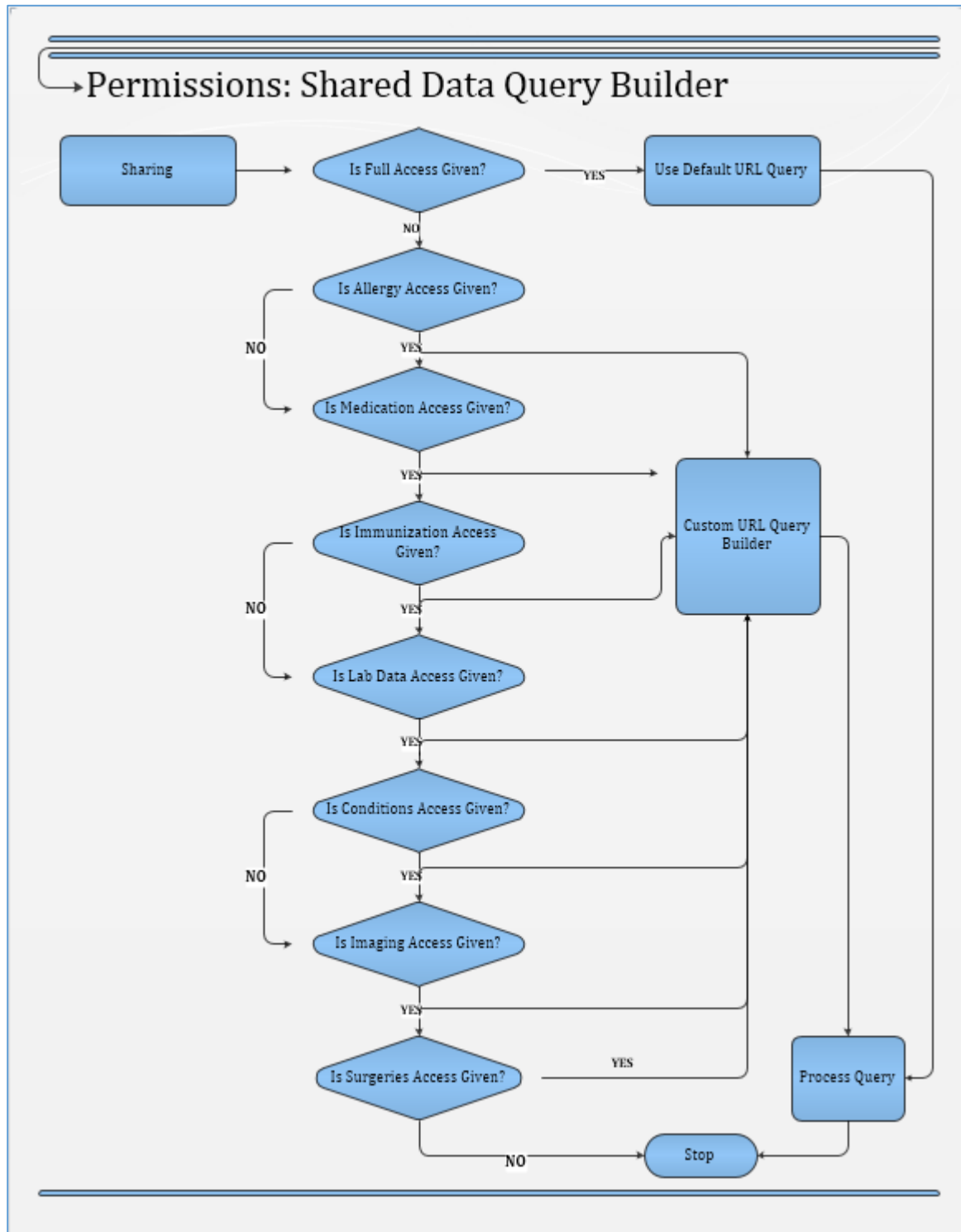
Personal Health	
Main Function	Sub-Functions
<p>PH.1 (Account Holder Profile) Manage PHR Account Holder demographics, preferences, Advance Directives, consent directives and Authorisations.</p>	<p><i>PH.1.1 (Identify and maintain patient record)</i></p> <p><i>PH.1.2 (Manage PHR Account Holder Demographics)</i></p> <p><i>PH.1.3 (Manage PHR Account Holder and Family Preferences)</i></p> <p><i>PH.1.5 (Manage Consents and Authorisations)</i></p> <p><i>PH.1.6 (Manage PHR Account Status)</i></p>
<p>PH.2 (Manage Historical Clinical Data and Current State Data) Statement: Historical health information as well as current health status should be captured and maintained in the health record.</p>	<p><i>PH.2.1 (Manage Patient Originated Data)</i></p> <p><i>PH.2.3 (Manage data and Documentation from External Clinical Sources)</i></p> <p><i>PH.2.4 (Produce and Present Ad Hoc Views of the Personal Health Record)</i></p> <p><i>PH.2.5 (Manage Current State Data Set)</i></p> <p><i>PH.2.5.1 (Manage Problem Lists)</i></p> <p><i>PH.2.5.4 (Manage Allergy, Intolerance and Adverse Reaction List)</i></p> <p><i>PH.2.5.5 (Manage Immunization List)</i></p> <p><i>PH.2.5.6 (Manage Medical History)</i></p>
<p>PH.6 (Manage Encounters with Providers) Statement: Manage information for scheduling, preparation, and assimilation of knowledge gained by encounters with providers.</p>	<p><i>PH.6.4 (Data and Documentation from External Clinical Sources)</i></p>
Information Infrastructure	
Main Function	Sub-Functions
<p>IN.1 (Health Record Information Management) Statement: Capture, store, secure, message, display and report PHR</p>	<p>IN.1.1 (Data Management)</p> <p>IN.1.2 (Synchronization)</p>

<p>information across PHR-S applications. Help ensure information entered by or on behalf of a PHR Account Holder is accurate. Facilitate appropriate identity checks before linking or transferring information between PHR records.</p>	<p>IN.1.3 (Present Ad-Hoc Views of the Health Record)</p> <p>IN.1.6 (Store and Manage Structured Health Record Information)</p>
<p>IN.3 (Security) Statement: Secure the access to a PHR-S and PHR information. Manage the sets of access control permissions granted within a PHR-S. Prevent Unauthorised use of data, data loss, tampering and destruction.</p>	<p>IN.3.4 (Non-Repudiation)</p> <p>IN.3.8 (Patient Privacy and Confidentiality)</p>

Appendix D: Application Process Flow Diagrams

Main Application Flow





Appendix E: Patient Tasks

Patient Tasks

1. Manage your Personal Health Record (PHR) data

You are a young professional living in Port Elizabeth. Your primary health provider (nmmu health services) has told you about a medical application that enables you to easily share your medical records with other medical practices across South Africa.

Part One

Complete the following:

a) Task One: Register to use the PHR mobile application

Create an account on the application, login with your new account.

b) Task Two: Search for nmmu health services in connect with them

Search for “nmmu” and share your account with them

c) Task Three: Add medical aid / insurance information

Use the application to add your insurance information.

d) Task Four: Add an allergy

Use the application to add an allergy to your record

e) Task Five: Add an immunization

Use the application to add an immunization to your record

f) Task Six: Add a condition

Use the application to add a condition your record

g) Task Seven: Add a Medication

Use the application to add a medication to your record

h) Task Eight: Backup your completed health record to the cloud

Once you finish backing up your information, NMMU health services will be able to view and manage your record.

Task Nine

You will be required to visit the NMMU health services department twice. The medical practice administrator will search for your record on a web application. You can ask him to carry out any of these tests:

- Measure your blood pressure
- Measure your weight
- OR any thing that you want.

He will then upload this information and you will be able to see it on your mobile device
END OF EVALUATION

Appendix F: Medical Practice Tasks

Participants will identify themselves as being there for “Personal Health Record Research Study”.

Procedure:

1. You will search for their names on the web application (URL provided).
2. Once a name is found, click on it to open up the patient chart.
 - a. View the PHR data of the given patient
 - b. Interact with the patient and agree on a medical exam that is to be carried out.
 - c. Upload the results of the medical examination.

Appendix G: Participant Consent Forms

RESEARCHER'S DETAILS	
Title of the research project	A Model for Managing Personal Health Records in South Africa
Reference number	H14-SCI-CSS-008
Principal investigator	Michael Kyazze
Address	Embizweni Building, Master's Lab
Postal Code	6031
Contact telephone number (private numbers not advisable)	27 41 504 2322

A. <u>DECLARATION BY OR ON BEHALF OF PARTICIPANT</u>		Initial
I, the participant and the undersigned	(full names)	
ID number		
<u>OR</u>		
I, in my capacity as	(parent or guardian)	
of the participant	(full names)	
ID number		
Address (of participant)		

A.1 HEREBY CONFIRM AS FOLLOWS:		Initial
I, the participant, was invited to participate in the above-mentioned research project		
that is being undertaken by	Michael Kyazze	
from	Department of Computing Sciences	
of the Nelson Mandela Metropolitan University.		

THE FOLLOWING ASPECTS HAVE BEEN EXPLAINED TO ME, THE PARTICIPANT:				Initial	
2.1	Aim:	The investigators are studying the usability of a mobile application that facilitates individuals to manage their personal health records. The information will be used to/for research purposes			
2.2	Procedures:	I understand that I will be asked to complete a series of tasks as presented to me			
2.3	Risks:	My participation in this study does not expose me to any risks			
2.4	Possible benefits:	There are no benefits			
2.5	Confidentiality:	My identity will not be revealed in any discussion, description or scientific publications by the investigators.			
2.6	Voluntary participation / refusal / discontinuation:	My participation is voluntary	YES	NO	
		My decision whether or not to participate will in no way affect my present or future academic performance / development / care / employment / lifestyle	TRUE	FALSE	
A.2 I HEREBY VOLUNTARILY CONSENT TO PARTICIPATE IN THE ABOVE-MENTIONED PROJECT:					
Signed/confirmed at		on		20	
Signature or right thumb print of participant		Signature of witness:			
		Full name of witness:			

IMPORTANT MESSAGE TO PATIENT/REPRESENTATIVE OF PARTICIPANT

Dear participant/representative of the participant

Thank you for your/the participant's participation in this study. Should, at any time during the study:

- an emergency arise as a result of the research, or
- you require any further information with regard to the study.

Kindly contact

Michael.Kyazze@nmmu.ac.za

Appendix H: Research Publication and Award

1. 2014 Global Tele-health Conference Paper Presentation

1

The Design and Implementation of a Ubiquitous Personal Health Record System for South Africa

Michael Kyazze, Janet Wesson & Kevin Naude
Department of Computing Sciences
Nelson Mandela Metropolitan University

3

Problem Context

5

Personal Health Records

- **Goal: Achieve ubiquitous access to personal health records**
- The American Health Information Management Association maintains a listing of existing PHR systems.
- The goal is to design and implement a successful PHR system in the SA context.

2

Introduction

Problem:

- Doctors experience difficulties in accessing medical information of new patients.
- Management of medical records is mostly institution-centred.
- Limited access to medical information may affect patients:
 1. Medical tests may need to be repeated;
 2. Doctors may prescribe drugs to which the patient is allergic.

4

Electronic Health Information

- **Electronic Medical Records (EMRs):** Issued by each medical practice for their record keeping purposes;
- **Electronic Health Records (EHRs):** A legal collection of various electronic medical records by a government body; and
- **Personal Health Records (PHRs):** Collection of various medical records that is initiated and maintained by an individual for purposes of continuity of care.

6

Requirements

Requirements were obtained from:

1. Health Level 7 PHR Functional Model
2. Review of existing PHR applications
3. Interview Studies with local medical practices to identify the main use cases and confirm the requirements

Health Level 7 Functional Model 7

Personal Health	PH.1 Account Holder Profile	★
	PH.2 Manage Historical Clinical Data And Current State Data	★
	PH.3 Wellness, Preventive Medicine, and Self Care	
	PH.4 Manage Health Education	
	PH.5 Account Holder Decision Support	
	PH.6 Manage Encounters with Providers	★
Supportive	S.1 Provider Management	
	S.2 Financial Management	
	S.3 Administrative Management	
	S.4 Other Resource Management	
Information Infrastructure	IN.1 Health Record Information Management	★
	IN.2 Standards Based Interoperability	★
	IN.3 Security	★
	IN.4 Auditable Records	★

Focus of this Research

Interview Study Findings 8

Two medical practices and a student medical centre were interviewed:

- They all have manual processes that enable them to manage their patient medical records.
- They all suffer from incomplete medical records for their patients especially new patients.
- They all emphasized the importance of patient confidentiality
- They were not keen on patients managing their own medical information, but they all agreed that a patient's self reported medical information is important.

Design 9

Ubiquitous PHR Management

Medical Practice: Web Enabled Desktop Computer
Patient: Mobile Device

1. Register Medical Practice
2. Search for a given Medical Practice
3. Connect your account with a medical practice
4. View Connected patients and manage their records

Secure Cloud database

PI: Personal Information
RMP: Registered Medical Practice
PHR: Personal Health Record

Implementation Tools 10

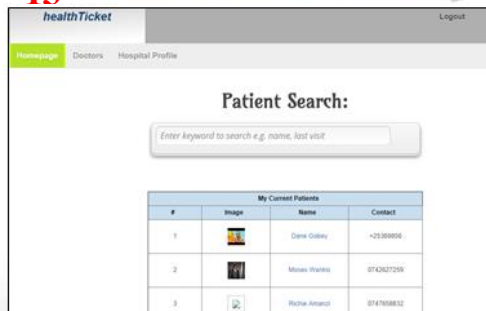
1. Android Mobile Application
2. Java web application hosted with OpenShift
3. MongoDB document database hosted on MongoLab
4. Cipher-Text Policy Attribute Based Encryption

Screen Designs 11

Screen Designs (2) 12

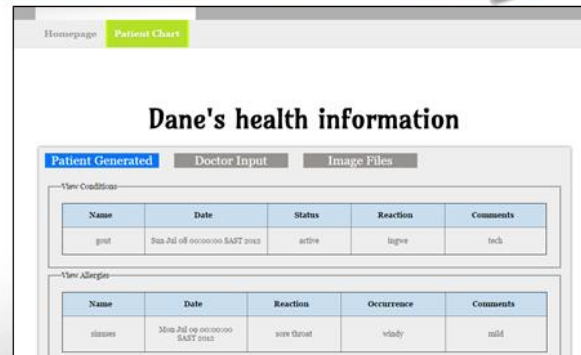
Medical Provider View

13



Example Patient Chart

14



Conclusions

15

- A field study was carried out with 12 participants and a local medical practice.
- Both the mobile and web applications were well received.
- The proposed system brings us closer to the realization of ubiquitous access to PHRs in SA.

Questions

16

- Any questions?
- Contact: kyazze@outlook.com

2. Best Presentation at the 2013 Interact African Masters Consortium



THE PRESENTATION TITLED

A Model for Managing Personal Health Records Using Mobile Devices in South Africa

BY

Michael Kyazze

WAS SELECTED TO RECEIVE THE

AWARD FOR THE BEST PRESENTATION AT THE AFRICAN MASTERS CONSORTIUM

HELD DURING THE INTERACT 2013 CONFERENCE

CAPE TOWN, SOUTH AFRICA

2-6 SEPTEMBER 2013

Paula Kotzé
CONFERENCE CHAIR

Janet Wesson
CONFERENCE CHAIR

Appendix I: Patient After-Scenario Questionnaire

A. Register to use the mobile application										
1. Overall, I am satisfied with the ease of completing the registration and login task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
2. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
3. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
General Comments										
B. Sharing your data with a health service provider										
1. Overall, I am satisfied with the ease of completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
2. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
3. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
General Comments										

C. Adding your personal health information to the application										
1. Overall, I am satisfied with the ease of completing the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
2. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
3. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
General Comments										
D. Syncing your health record to a the cloud server										
1. Overall, I am satisfied with the ease of completing the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
2. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
3. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
General Comments										

E. Viewing medical data uploaded by medical practices									
4. Overall, I am satisfied with the ease of completing the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
5. Overall, I am satisfied with the amount of time it took to complete the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
6. Overall, I am satisfied with the support information when completing the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
General Comments									

Appendix J: Patient Post-Test Questionnaire

A. Biographical data										
1. Gender: Male, Female.....										
2. Age range: 18-20 years....., 21-29 years....., 30-39 years....., 40-49 years....., 50+.....										
3. Occupation:										
4. Android Experience: 0-6 months....., 1-2 years....., > 2 years.....										
B. Cognitive load										
4. Mental demand: How mentally demanding were the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
5. Physical demand: How physically demanding were the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
6. Temporal demand: How hurried or rushed was the pace of the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
7. Performance: How successful were you in accomplishing what you were asked to do?										
	Very Low	1	2	3	4	5	6	7		Very High
8. Effort: How hard did you have to work to accomplish your level of performance?										
	Very Low	1	2	3	4	5	6	7		Very High
9. Frustration: How insecure, discouraged, irritated, stressed, and annoyed were you?										
	Very Low	1	2	3	4	5	6	7		Very High
C. Overall satisfaction										
1. Overall, I am satisfied with how easy it is to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
2. Overall, I am satisfied with the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
3. It was easy to learn to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
4. It was simple to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
D. Usability										

1. I can effectively find medical practices using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
2. I was able to share my personal health records effectively using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
3. I was able to selectively share my personal health records using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree

4. I felt that my personal health records were secure when using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
5. The system has all functions and capabilities than enable me to securely manage personal health records										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
6. I can effectively browse my personal health records collection using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
7. I was able to browse my personal health records quickly using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
8. I was able to browse the medical practices who have access to my personal health records										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree

E. General

1. Identify the most positive aspect of the system										
2. Identify the most negative aspect of the system										
3. Please provide any general comments or suggestions for improvement										

Appendix K: Medical Practice After-Scenario Questionnaire

A. Searching for patients on the system										
10. Overall, I am satisfied with the ease of completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
11. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
12. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
General Comments										
B. Viewing a patient's self-reported data										
7. Overall, I am satisfied with the ease of completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
8. Overall, I am satisfied with the amount of time it took to complete the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
9. Overall, I am satisfied with the support information when completing the task										
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree	
General Comments										

C. Adding a patients consultation data									
4. Overall, I am satisfied with the ease of completing the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
5. Overall, I am satisfied with the amount of time it took to complete the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
6. Overall, I am satisfied with the support information when completing the task									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
General Comments									

Appendix L: Medical Practice Post-Test Questionnaire

A. Cognitive load										
13. Mental demand: How mentally demanding were the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
14. Physical demand: How physically demanding were the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
15. Temporal demand: How hurried or rushed was the pace of the tasks?										
	Very Low	1	2	3	4	5	6	7		Very High
16. Performance: How successful were you in accomplishing what you were asked to do?										
	Very Low	1	2	3	4	5	6	7		Very High
17. Effort: How hard did you have to work to accomplish your level of performance?										
	Very Low	1	2	3	4	5	6	7		Very High
18. Frustration: How insecure, discouraged, irritated, stressed, and annoyed were you?										
	Very Low	1	2	3	4	5	6	7		Very High
B. Overall satisfaction										
5. Overall, I am satisfied with how easy it is to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
6. Overall, I am satisfied with the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
7. It was easy to learn to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
8. It was simple to use the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
C. Usability										
2. I can effectively find medical practices using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
9. I was able to share my personal health records effectively using the system										
	Strongly Disagree	1	2	3	4	5	6	7		Strongly Agree
10. I was able to selectively share my personal health records using the system										

	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
--	-------------------	---	---	---	---	---	---	---	----------------

11. I felt that my personal health records were secure when using the system									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
12. The system has all functions and capabilities than enable me to securely manage personal health records									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
13. I can effectively browse my personal health records collection using the system									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
14. I was able to browse my personal health records quickly using the system									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree
15. I was able to browse the medical practices who have access to my personal health records									
	Strongly Disagree	1	2	3	4	5	6	7	Strongly Agree

D. General									
4. Identify the most positive aspect of the system									
5. Identify the most negative aspect of the system									
6. Please provide any general comments or suggestions for improvement									

Appendix M: Patient and Medical Practice Interaction Diagram

