Designing an Architecture for Secure Sharing of Personal Health Records - A Case of Developing Countries

RICHARD SSEMBATYA

MSc. Computer Science (MUK), BSc. Computer Science (Hons) (MUST)

Thesis

Submitted in Fulfilment of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY
Department of Computer Science, Faculty of Science
UNIVERSITY OF CAPE TOWN

Supervised by: Dr. Anne V.D.M. Kayem & Prof. Gary Marsden

August 2014

“May the mind of Christ my Savior, live in me from day to day.

By His love and power controlling all I do and say”

- *Kate Barclay Wilkinson*

Dedicated to my late father Joseph, late grandmother Mary and the Ssembatya family

"No one who achieves success does so without acknowledging the help of others. The wise and confident acknowledge this help with gratitude"

- *Alfred North Whitehead*

ACKNOWLEDGEMENTS

Many people have accompanied me during this journey of adventures and discovery. Travelling together makes a journey more fun, more creative and more challenging. This experience has given me the opportunity to meet people from backgrounds such as health, education and political background. These people have guided me, supported me, and encouraged me in one way or the other. Many people deserve my greatest gratitude for having made this journey possible.

First, I would like to thank the Almighty Lord for making ways where they seemed to be no way. Without his mercy, protection and love, this journey would never been a success.

Special thanks go to Hasso Plattner Institute (HPI) for the generous contribution towards this journey, especially at the most prestigious University - University of Cape Town. This journey would not have been possible without your support.

My sincere thanks also go to my supervisors: Prof. Gary Marsden and Dr. Anne V.D.M. Kayem, for your excellent guidance, motivation, enthusiasm, and providing me with an excellent atmosphere for doing this research. I could not have imagined having better supervisors for this journey.

Besides my supervisors, I would like to thank the rest of the Department of Computer Science lecturers, at the University of Cape Town, for their encouragement, insightful comments, and thought-provoking questions.

My greatest appreciation and friendship goes to my closest friend Sylvia, who was always a great support in all my struggles and frustrations in this journey. Thanks for questioning me about my ideas and helping me think rationally. Cheers to Auntie Sylvia for being a great reliable person to whom I could always talk about my problems and excitements.

I would also like to thank my princess Tracy and my guy Travis. They were always supporting and encouraging me with their best wishes and prayers.

My sincerest thanks and gratitude go to the administration of Allan Galpin Health Centre (AGHC) for allowing me conduct my studies at their premises. Special thanks go to Christine, Lydia, Martin and Geoffrey.

I thank my fellow colleagues in ICT4D lab, University of Cape Town: Grace, Ntwa, Maletsabisa, Chao, Mgala, Ronke, Hajji, Thomas, Pierre, Fritz, Nini and Sarah, for the stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the fun we have had during this journey.

Lastly, may the good Lord reward all those persons whose names I have not mentioned here for their support during this journey. You played a significant role for which I am grateful to say "Thank You".

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

While there has been an increase in the design and development of Personal Health Record (PHR) systems in the developed world, little has been done to explore the utility of these systems in the developing world. Despite the usual problems of poor infrastructure, PHR systems designed for the developing world need to conform to users with different models of security and literacy than those designed for developed world.

This study investigated a PHR system distributed across mobile devices with a security model and an interface that supports the usage and concerns of low literacy users in developing countries. The main question addressed in this study is: *"Can personal health records be stored securely and usefully on mobile phones?"*

In this study, mobile phones were integrated into the PHR architecture that we/I designed because the literature reveals that the majority of the population in developing countries possess mobile phones. Additionally, mobile phones are very flexible and cost efficient devices that offer adequate storage and computing capabilities to users for typically communication operations. However, it is also worth noting that, mobile phones generally do not provide sufficient security mechanisms to protect the user data from unauthorized access.

The research question was addressed through a systematic review of healthcare systems, a survey of healthcare consumers and providers, and usability experimentation. The review of health systems was conducted to refine the problem. A survey of end-users (patients and healthcare givers) was carried out, and the findings were useful in understanding the current state of practice of personal health records, understanding patients' needs and requirements, and deciding on the components of the PHR system to be implemented. The design, development, implementation and evaluation of the PHR system were achieved through a Patient-Centred Design (PCD) approach and Human Access Points (HAP) technique. Data security was implemented by incorporating in addition, an Identity-Based Encryption (IBE) architecture.

The laboratory evaluation results of the mobile phone-based PHR system demonstrate that the proposed IBE can be extended to mobile phones to secure PHRs beyond the hospital's server domain. Additionally, the usability evaluation results reveal that the system is useful to patients in: supporting their memory; confirming personal health records and accuracy; learning about their conditions regularly; and minimising medical jargons. Moreover, none of the medical practitioners reported any concern. Instead, the medical practitioners recalled their experience with the system in a positive light: supports medical-decision making; improves relationship with their patients;

and provides continuity of patients' care when the healthcare server is offline due to frequent power outages and/or unreliable Internet connections.

"A dream doesn't become reality through magic.
It takes sweat, determination and hard work"
- Colin Powell

CHAPTER ONE: INTRODUCTION

1. Introduction

One of the foremost challenges facing developing countries[1] is the struggle to raise people's standard of living, within their limited resources (Montgomery & Hewett, 2005; Sachs, 2008). It is also recognised that the response to this challenge must be universal, including cultures and societies of human beings in developing countries. This was also clearly articulated in the Millennium Development Goals (MDGs[2]) statement that was endorsed by the member states of the United Nations.

The MDGs place a central focus on peoples' health, in recognition of the fact that improvements in health are vital to break the poverty trap of the world's poorest countries. A significant number of the MDGs are explicitly about health: reducing the child mortality rate by two-thirds by 2015; reducing the maternal mortality rate by three-quarters by 2015; controlling the great pandemic diseases of Human immunodeficiency virus infection / acquired immunodeficiency syndrome (HIV/AIDS), malaria and tuberculosis; giving access to safe drinking-water and sanitation; and alleviating hunger and under nutrition (Sachs, 2004). Furthermore, the first Millennium Development Goal of reducing extreme poverty among the population cannot conceivably be accomplished if the health goals are not achieved. Sachs (2004) acknowledged that societies burdened by sicknesses and dying individuals cannot escape from poverty.

Similarly, the UN research agenda also highlighted public health as the first indicator to improve peoples' standard of living. (United Nations reports 1954, 1961). According to

[1] The classification of countries into the category of 'developing countries' is both complex and controversial (Sundén & Wicander, 2006:57-64, esp. 59). Developing countries constitute over 70 per cent of the world's population. The terms developing countries (DC) will be used in this thesis as the terms to represent countries with various challenges such as poor infrastructure, poverty, unreliable and intermediate main electricity in addition to other information and communication technology (ICT) constraints such as little or no Internet bandwidth and lack of user expertise

[2] Millennium Development Goals. http://www.un.org/millenniumgoals/, 2005.

Investopedia dictionary, the standard of living of individuals does not only depend on the income people themselves earn, but also to affordable access to quality healthcare. Other factors that determine the standard of living of individuals include: cost of goods and services, infrastructure, incidence of disease among others. Thus, the standard of living is closely related to quality of life.

Sachs (2008) described that public health is one of the basic services that can greatly improve people's standard of living in developing countries. However, several challenges such as scarcity of financial resources and infrastructure, combined with ineffective health structures and mismanagement are among the critical constraints of health services in developing countries (Sachs, 2004).

Considering these challenges, it is essential to find a sustainable way for the undeveloped communities to achieve a healthy standard of living. In some countries, an optimistic vision has emerged that undeveloped communities might employ digital technology in a sustainable way to help them achieve many development goals. This is referred to as Information and Communication Technology (ICT) for Development, or ICT4D. Meaning, providing several billion people in the undeveloped communities with sustainable technology to achieve development goals such as improved access to healthcare services (Heeks, 2008).

For example, in the last 50 years, advances in computing and other information and communication technologies have transformed the way individuals create and share information. Within healthcare, ICTs have spurred an empirical revolution to electronic health or E-health. The potential of E-health systems in the management of healthcare information is also emphasized by the following quote from Braa and Blobel (2003);

> *"Without reliable and relevant E-health system, health care managers and providers cannot improve the quality of health services, optimally allocate resources or address epidemics such as HIV/AIDS."*

We are therefore interested in how e-health might address healthcare needs in the developing world effectively. In addition, we are interested in determining whether or not the application of ICT4D in healthcare management in the developing world might realise similar improvements to the ones experienced in the developed world.

1.1 E- Health

Electronic health or E-health emerged in the early 21st century to "introduce" the use of electronic information and communication technology in the health sector (Harrison & Lee 2006). While some scholars associate E-health solely with computers, Harrison and Lee (2006) broadly used the term to describe any electronic exchange of health related information, analysed through electronic media to improve the efficiency and effectiveness of healthcare delivery. Thus, E-health is often used to describe anything related to computers and medicine (Kwankam, 2004; Deluca & Enmark, 2002; Kind & Silber, 2004). The concept of E-health is used to describe the application of ICT to meet the needs of citizens, policy makers, healthcare professionals and providers (Silber, 2003). Other definitions associate E-Health strictly with the Internet, focusing on the growing importance of the Internet in health transactions. Grimson (2001a) described E-health as an emerging field of medical informatics, where delivery of health services and information is done through Internet technologies. Grimson et al. (2001) defines E-health in terms of medicine plus communication plus information plus society. The Health Telematic Working Group (2003) describes E-health as the use of ICTs with the Internet to:

- Connect healthcare and information providers, citizens and government;
- Inform, educate and empower citizens, healthcare professionals, managers and policy makers; and
- Improve the quality and management of health data, healthcare delivery and health system management.

Thus, ICTs play an important role in improving the efficiencies and effectiveness of healthcare service delivery. Through the use of ICTs such as mobile phones, healthcare providers and patients can potentially monitor, control and provide health information as well as communicate more effectively across organisational hierarchies (Bhatnagar, 1992; Braa & Blobel, 2003; WHO, 2005; Chandrasekhar & Ghosh, 2001).

Despite the many benefits of having E-health systems in place, the development of appropriate and scalable Electronic Health Record (EHR) systems in developing countries has proved to be difficult because of certain limitations inherent to the technological infrastructure. Current healthcare services and practices in most areas of developing countries are primarily paper-based (Fraser et al., 2007; Anokwa, Allen, & Parikh, 2008; Luk, Zaharia, Ho, Levine, & Aoki, 2009). Paper-based health record systems pose many disadvantages, such as incorrect recording of diagnoses, unavailability and loss of patient information, delays in accessing the information and space limitations for record-keeping (Anokwa et al., 2008; Luk et al., 2009). Additionally, due to infrastructural constraints, such as intermittent power and Internet connectivity, the introduction of computing technologies to automate these processes is equally challenging.

In a related study that was carried out to identify how the current healthcare systems work in developing countries, it was observed that the process of using patient data is mainly paper-based. When providers see patients, paper-based forms are completed to document the encounter. Every few days, the encounter along with laboratory data is manually entered into the EHR system and then returned to the patient's record. Upon a return visit, the provider reviews the patient's record on paper using the previous encounters to guide decision making. Most EHR systems in developing countries focus on reporting aggregate statistics to the stakeholders (Anokwa, 2010).

Additionally, despite the high level of patient desire to protect their records, health systems in developing countries do not adequately protect patients' records. For example, a study we conducted at Allan Galpin Health Centre (AGHC) Uganda reveals that all the clinical employees including doctors, nurses, receptionists and technicians have access to all the health records for all the patients in the EHR system.

In a subsequent study, a systematic review of EHR systems designed for developed countries revealed a number of open research problems in respect to developing countries (Mugwanya 2013). Some of the ones identified include the following;

1. **EHR systems are online only:** The majority of EHR systems require online access control decisions. Relying solely on online access control systems is limiting, particularly in developing countries where access to the servers is frequently disrupted by frequent power outages and limited bandwidth among other constraints. When the server fails or becomes unavailable, access control decisions cannot be made, making PHRs unreachable.
2. **Provider-centric environment:** Most EHR systems are designed to facilitate access for healthcare providers rather than patients. As such, a patient has little or no access to his/her records. Personal Health Record (PHR) systems such as Microsoft

HealthVault[3], Indivo[4] and Dossia[5] empower users with some access but the access must be online. In addition, all the tools we found are developed with user contexts in the developed world and thus may not represent the needs of the users in developing world. Most EHR systems are desktop centric and are not accessible to the majority of the population in developing countries.

1.2 Motivation and Problem Definition

It is interesting to note that mobile phones have replaced personal computers in terms of information access and communication support in developing countries (Parikh & Lazowska, 2006). Almost four in every five people in developing countries own a mobile phone for information access, exchange and transfer (ITU, 2013). The transfer and exchange of information are used in the context of applications for health purposes (Olla & Tan, 2006; Rashid & Elder, 2009), education (Sharples, Corlett, & Westmancott, 2002; Seppälä, P., & Alamäki, 2003; Rashid & Elder, 2009) and banking (Barnes & Scornavacca, 2004; Laukkanen & Lauronen, 2005).

The handheld computers (mobile phones) have been demonstrated as a tool that improves healthcare delivery in rural areas of developing countries (Ho, Owusu, & Aoki, 2009; Hartung et al., 2010; Anokwa et al., 2012). The keypad familiarity and extended battery use makes it a design choice for millions of healthcare givers and patients in developing countries (Parikh & Lazowska, 2006; Anokwa et al., 2012). The growth of the wireless infrastructure in most parts of rural areas, and the reducing cost of the device provides an opportunity to bootstrap computing in the developing world.

Rashid and Elder (2009) identified several reasons why mobile phones are considered important for rural healthcare. First, beyond basic connectivity, mobile phones offer benefits such as mobility and security to owners (Donner, 2006). Secondly, because of their unique characteristics, there is no need to rely on physical infrastructure such as roads, and the base-stations can be powered using the provider's own generators in places where there is no electrical grid (Economist, 2008). In addition to voice communication, mobile phones allow for the transfer and exchange of health information, which can enable physicians to remotely

[3] https://account.healthvault.com/help.aspx

[4] http://indivohealth.org/

[5] http://dossia.org

monitor patients' health, and enable individuals to manage their own health more easily (Avancha, Baxi, & Kotz, 2012; Benelli & Pozzebon, 2010; Han, Park, & Lee, 2008). These features have made mobile phones a better suited device for rural developing World than a conventional PC (Parikh & Lazowska, 2006).

While mobile phones are very flexible and cost efficient devices that offer storage capabilities to users, they generally do not provide sufficient security mechanisms to protect the data on which users operate. This is mainly due to the architectural shortcomings of their design (Dmitrienko, Hadzic, Löhr, Winandy, & Sadeghi, 2011). Although some cellular phone operating systems such as Google Android offer good security mechanisms, such as application-oriented access control, for protecting mobile data (Google Android, 2010), these security mechanism implementations are still known to be vulnerable to attacks that stem from the fact that the stored data is not adequately protected from unauthorised access (Dmitrienko et al., 2011).

Some attacks on mobile phones have demonstrated their vulnerabilities (Aggarwal & Vennon, 2010), indicating that security of the data stored on the mobile phone is important especially when a user is working with privacy-sensitive data such as personal health records on the device (Dmitrienko et al., 2011; Hupperich et al., 2012; Dmitrienko, Hadzic, Löhr, Sadeghi, & Winandy, 2013).

Likewise, while the stationary servers in the healthcare telematics may be protected by additional security architectures and hardware components such as specialised firewalls and gateway routers, the situation gets worse when data is downloaded to the mobile phone (Dmitrienko et al., 2011). This is due to the fact that the limited processing and memory capabilities of mobile phones are a hindrance in supporting these architectures. As a result, the data downloaded and stored on the mobile phones stays unprotected, and therefore accessible by unauthorised parties.

In this dissertation, I propose a secure architecture for handling Personal Health Records (PHRs) on mobile phones. Additionally, I examine the opportunities of using mobile phones to improve secure access and sharing of health information in rural areas of developing countries. Thus, the thesis is framed within the research area of ICT for development or ICT4D, which is concerned with "Understanding precisely how ICTs can make a difference to the lives of the poor and marginalised" (Unwin, 2009) and, "how ICTs can be applied to make it useful to the poor" (Heeks, 2008).

1.3 Adversary Model

In this study, I consider a traditional healthcare scenario in which patients' electronic health records (EHRs) are stored on a local server of the healthcare provider, e.g., hospital. I assume that patients[6] are equipped with mobile devices such as mobile phones on which they can use to download and store their Personal Health Records (PHRs). Since patients' health records are originally stored at the hospital server, mobile phones communicate with the server via wireless network connections through a mobile phone-application using standard web browsers on the mobile phone. Figure 1.1 below depicts the scenario.

The patient's health record, when stored on a mobile phone is considered to be a high security sensitive piece of information. In many countries such as Angola and South Africa this sort of data is protected under strong privacy laws. Therefore, it is important to ensure that the mobile data is adequately protected from unauthorised access. In Figure 1.1 below, an adversary may try to eavesdrop or manipulate patient's records. Sunyaev, Leimeister, and Krcmar, (2010) affirmed that the majority of end-user devices such as mobile phones are typically the least secured devices in the healthcare infrastructures. Therefore, an adversary may most likely try to attack the mobile phone or its communication connection to the server in order to illegitimately access patient's medical records. Thus, the following research questions were investigated.

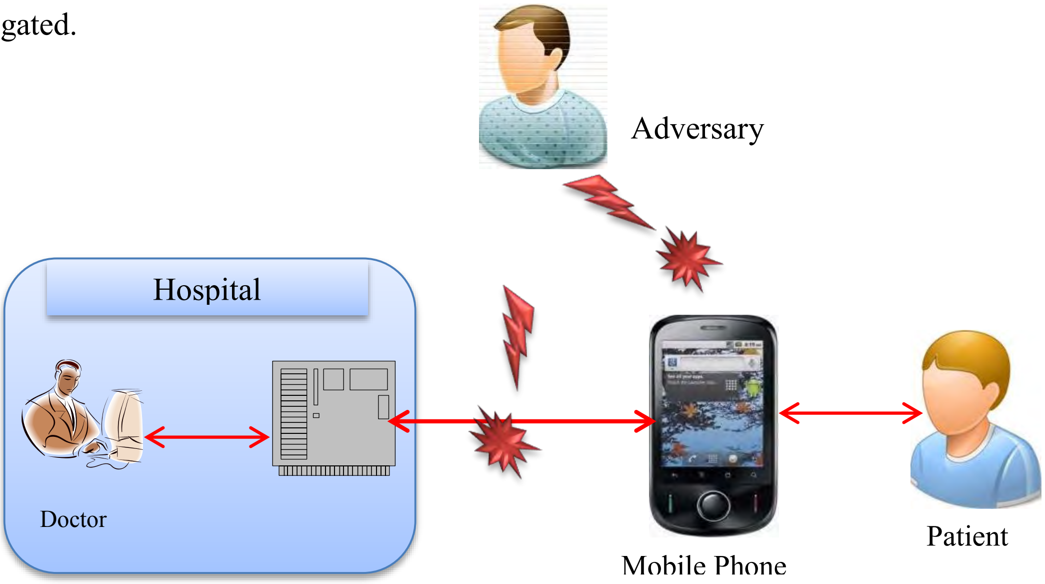


Figure 1.1: Use Case and Adversary Model

[6] In relation to this study, a patient is any recipient of health care services

1.4 Main Research Question

Can personal health records be stored securely and usefully on mobile phones?

1.4.1 Specific Research Questions

1. Can I provide an access control architecture that can be used to secure patient's records on mobile phone?
2. Can the proposed architecture be usable on mobile phone without interfering with the 'normal' use of the device in terms of its efficiency, performance and resources management?
3. How useful are the mobile phone-based PHR systems to the users including healthcare professionals and the patients?

The first research question provides the design of an access control framework that protects personal health records on mobile phone, based on the findings of a three-month contextual study with patients at Allan Galpin Health Centre (AGHC). The design aims to provide secure access of patients' records even when hospital servers are offline, due to frequent power outages and/or unreliable Internet connections. The second research question investigates the possibility of deploying the proposed architecture to mobile phones without interfering with the 'normal' use of the device, considering mobile phone constraints such as memory and processing limitations. Finally, the last research question examines the usefulness of mobile phone-based PHR systems in developing countries, and the perceptions that patients and healthcare workers have towards these systems.

1.5 Contributions of the Thesis

In summary, the following are the research contributions that are described in this dissertation;

Identification of Systemic Technology Gaps in EHR Systems Designed for Developed Countries. Based on a systematic review of EHR systems conducted as part of this study, I affirm that EHR systems designed for developed countries cannot be adapted for implementation in developing countries. The failure of adoption is attributed to factors such as: designed for online access control, and/or desktop platform specific, which majority of the population in developing countries do not have access.

An Access Control Framework (ACOF) that Protects Patients Records on Mobile Phone. Based on a contextual study covering three months of field work with patients at AGHC, and a one month participatory design study that include the Human Access Points (HAP), I proposed and presented the ACOF architecture that protects patients' records beyond the hospital's trust boundaries.

M-Health App System: The M-Health App system is a component of ACOF, implemented on mobile phone to support secure sharing of PHRs when the hospital servers are offline. The M-Health App system is a novel PHR system for mobile phones. Motivated by the earlier paper-based designs and patient-user requirements, the system enables patients to securely download and update their medical records onto the mobile phone in order to support offline access.

Evaluation of M-Health App System for Performance and Usability. I provide the evaluation of M-Health App system and describe the results of usability and laboratory experiments. The results of these experiments demonstrate two key contributions: (1). Mobile phones can be used to provide efficient and secure storage of PHRs. (2). Suitably adapted mobile phone-based PHR system can address health needs of low-literacy and technology-constrained users in developing countries.

1.6 Outline of the Dissertation

The rest of this dissertation is structured as follows: In chapter 2, we present the findings of our initial review of EHR systems. The literature reveals that despite the potential of EHR systems to address the challenges facing healthcare systems in developing countries, the majority of EHR systems designed for developed countries cannot be adapted for implementation in developing countries. The failure of adoption is attributed to the fact that most EHR systems require online access control decision. When the server/database is unavailable, for example due to frequent power outages that is common in developing countries, access control decisions cannot be made, making health records unreachable.

In chapter 3, I further examine the literature related to electronic health records (EHRs), Personal Health Records (PHRs), privacy and security models, usability in security domain, and conclude that Identity-Based Encryption (IBE) can be a good choice to protect personal health records stored on mobile phone. The choice of IBE is derived from a number of benefits: it is inexpensive to operate, and supports off-line capabilities; it supports a wide range of authentication methods to ensure user identity; and finally, it offers basic and less consuming processing capabilities on mobile phones to support secure storage of personal health information.

In chapter 4, I describe patient's views and requirements towards mobile phone-based PHR systems based on the finding of a three-month contextual inquiry with patients at AGHC. Additionally, I explore further with healthcare providers the information patients can have on mobile phones. The chapter concludes that although patients support the idea of having their personal health records stored on mobile phones to support portability and control, they are also concerned about cases of unauthorised access and difficulty of use.

In chapter 5, I present a participatory design study conducted in collaboration with the Human Access Points (HAP). The chapter documents the design activities, and concludes with the results of formative evaluation with the final beneficiaries.

In chapter 6, I propose and present the implementation of ACOF that protects patients' health information on mobile phones. Motivated by the earlier paper-based designs and patients' requirements, the framework enables secure sharing of PHRs beyond the hospital's trust boundary. Additionally, the chapter describes the design and implementation of the mobile phone-based PHR system called M-Health App system, which is an ACOF component. Contrary to other systems, the M-Health App system incorporates the "push model" where patients can periodically download and update their health records to the mobile phone with minimal user intervention. However, only users with a PIN that satisfies the policy are able to decrypt the records.

In chapter 7, I present evaluation activities and results obtained after M-Health App system evaluations. Three types of evaluations were conducted: laboratory evaluations that don't involve end-users, laboratory evaluations that involve end-users, and finally the field study evaluation. The results of the evaluation indicate that mobile phones can be used to provide efficient and secure storage of PHRs, and the personal health records stored on mobile phone are useful to patients and healthcare professionals.

In chapter 8, I conclude the dissertation and describe the research contributions, limitations and ideas for future work.

"As mobile ownership passes 4 billion,
the ICT4D Community is looking to mobile data."

- *Jonathan Donner*

CHAPTER TWO: CHALLENGES OF ADOPTING STANDARD EHR SYSTEMS IN DEVELOPING COUNTRIES

2. Introduction

This chapter provides a conceptual grounding to the research in this thesis, and defines the key research gaps that hinder the adoption of standard Electronic Health Record (EHR) systems in developing countries. The chapter describes healthcare barriers and information challenges in developing countries, and the digital divide. Furthermore, an overview of ICT4D and ICT4H are presented and lastly, the analysis of EHR systems. Based on this analysis, the chapter sets out a research agenda for the thesis.

2.1 Overview of EHR Systems

Electronic Health Record (EHR) systems are a popular mechanism for accessing health records, and have contributed towards improved and cost-effective healthcare management. Greenhalgh, Potts, Wong, Bark and Swinglehurst (2009) described an EHR system as a container holding information about the patient, and a tool for aggregating medical data for secondary uses (e.g. billing and auditing). Thus, the EHR system is designed primarily to capture patient's data, and represent information about the patient.

Black et al. (2011) described three main overlapping functions of EHR Systems;

- It supports the entire patient history to be viewed without the need to track down the patient's previous health record volume.
- It reduces the duplication of patients' records since there is only one modifiable file
- Minimises issues of lost health procedures and/or paperwork; and assists in ensuring that patients' records are accurate, appropriate and legible.

2.2 EHR Systems Background

Over time, researchers have made significant efforts to design and implement EHR systems of which some are employer sponsored (Dossia, sponsored by Wal-Mart, BP and AT&T),

provider sponsored (MyHealtheVet, sponsored by the United States Department of Veterans Affairs), and others are independent products (Microsoft HealthVault and Google Health, which were developed for profit making and open source projects respectively). However, the development of appropriate and scalable EHR systems in developing countries has been difficult to achieve (Omary, Lupiana, Mtenzi, & Wu, 2009; Tierney et al., 2010; Kalogriopoulos, Baran, Nimunkar, & Webster, 2009). The literature reveals many EHR systems that have not survived the test of time. Such systems include MEDCAB (Kamadjeu, Tapang, & Moluh, 2005) and FUCHIA (Tassie et al., 2002). All the available literature indicates that these systems are no longer actively in use or development. Hsu et al. (2005) recommended that there is a need for more research to determine potential reasons for failures and disparities as well as the implications of these failures/disparities on clinical out (Hsu et al., 2005).

Similarly, with the explosion of open-source EHR systems, more patients and physicians in developed countries are shifting towards accessing health information online. The $34 billion of incentives provided by the American Recovery and Reinvestment Act (ARRA) (2009) has greatly increased the development of open-source EHR systems in developed countries. The ARRA further stresses that healthcare providers should deploy EHR systems that are certified for "meaningful use[7]" criteria, which includes the implementation of access control (Smith et al., 2010). The intent of meaningful use criteria is to ensure that EHR systems can interoperate with other systems in order to enable electronic exchange of health information in accordance with all laws and standards.

While previous studies have widely documented the success and failure factors of information and communication technology (ICT) solutions in developing countries, there appears to be a gap in specifically answering the question regarding whether online health services designed for developed countries can be adopted for EHR systems in developing countries. Studies conducted by Fraser et al. (2005), Mars and Seebregts (2008), Yogeswaran and Wright (2010), Abdul (2008), Boonstra and Broekhuis (2010), and Forster et al. (2008) deal with broader issues of adoption such as technology investments, early stakeholder's participation and training. Other studies focus on policy and regulatory issues for EHR systems and given less attention to technological barriers (Coleman, 2010; Jacucci, Shaw, & Braa, 2006). In addition,

[7] http://www.healthit.gov/. Meaningful use is the set of standards that governs the use of electronic health record systems.

most studies have been conducted for developed countries (Greenhalgh et al., 2010; Sanders et al., 2012; Gagnon et al., 2009; McGinn et al., 2011; Thakkar & Davis, 2006). From the perspective of the health digital divide, the available literature does not yet seem to adequately answer whether health services designed for developed countries can be adopted in developing countries. Therefore, the aim of this chapter is to assess the potential and applicability of the current EHR systems in developing countries. We classify and summarize EHR systems and provide a framework to extract assertions and provide guided decisions. A set of assessment criteria was established to ascertain the degree to which the evaluated systems address technology constraints in developing countries, NIST[8] meaningful use and CCHIT[9] certification. Using these evaluation criteria, the researcher evaluated 19 EHR systems extracted from online search databases.

2.3 Rural Healthcare Barriers and Information Challenges

In this section, we discuss some of the challenges faced by the people living in rural areas of developing countries. These challenges are based on personal observations drawn from our experiences in rural Uganda, and literature review.

2.3.1 Frequent Power Outages

The availability of reliable electric power supplies is a precondition for the functioning and provision of quality healthcare. However, many developing countries experience significantly low levels of electrification (Parikh & Lazowska, 2006). The power grid in developing countries is extremely unpredictable. There is load-shedding both in urban and rural areas of developing countries in order to conserve energy for other areas. An electric generator is always necessary for each healthcare provider, which creates additional expenses that many providers in developing countries cannot afford or are reluctant to bear.

In relation to Uganda, the expansion of ICTs has been limited due structural challenges such as limited electrical grid. The national survey conducted by International Energy Agency (IEA) (2009) reveals that 96 percent of rural households in Uganda lack access to electricity. Users travel many kilometres to charge their phones and often receive poor service from the charging

[8] http://www.nist.gov
[9]http://www.cchit.org

station. The lack of accessible sources of electricity for recharging a phone is a huge constraint to the majority of the population leaving in rural areas of Uganda.

2.3.2 Intermittent Connectivity

Due to the poor ICT infrastructure, the majority of areas in developing countries cannot support Internet deployment, which in turn hinders electronic records (Omary et al., 2009). In some rural areas with Internet connections, low-quality copper wire is always used. Internet connections over these links are slow and frequently disconnected. However, with the penetration of cellular technologies, wireless networks will eventually make connectivity more accessible even to the poor (Parikh & Lazowska, 2006).

2.3.3 Lack of Centralised Services

In the developed world, the provision of services such as healthcare services is centrally organised to ease the distribution of healthcare services. Traditionally, the hospital server runs the EHR application to support the provision of healthcare services. However, this is not possible in many countries in developing world due to constraints described in sections 2.3.1 and 2.3.2.

2.3.4 Long Travels for Healthcare Services

One of the most often cited attributes of rural areas that affects service delivery in healthcare is the large distances between residences and healthcare providers. Several transfers may be required to travel from one place to another. However, due to poor road systems coupled with inadequate and unaffordable transport, it is always difficulty to reach the healthcare facility in a required time. Additionally, accessing healthcare services usually means long waiting times due to traditional practices of paper-based records (Omary et al., 2009).

2.3.5 Limited Education

The majority of countries in developing World have low quality schools, which often forces children to abandon schooling at an early stage (Parikh & Lazowska, 2006). Similarly, the high demand for agricultural farming has also contributed highly to school dropout. Many people living in rural areas are illiterate (Rouvinen, 2006). The UNESCO institute for statistics estimated that more than half of the adult population in developing countries were functionally illiterate by the year 2008 (UNESCO Institute for Statistics, 2010). The high level of illiteracy rate significantly contributes to the disease burden of poor countries, and reinforces health inequalities and digital divide (Kickbusch, 2001).

In an effort to fulfil the Millennium Development Goals (MDG), the government of Uganda introduced free primary education in 1997 that was extended up to 4 children per family. The government took into consideration marginalized groups of the disabled and female children to be included in this figure. Enrolment in primary schools swelled from 2.9 million to 5.6 million and today stands at over 8.3 million (Kagoda, 2012).

In 2010, the overall literacy rate was 73% among persons aged 10 years and above. More men were literate (79%) compared to women (66%) (The state of Uganda population report, 2013).

2.4 E-Health and Digital Divide

In the context of this study, developing countries are countries with various challenges such as those described in section 2.2, in addition to other Information and Communication Technology (ICT) constraints, such as a lack of user expertise. When compared to developed countries, the gap is described as the digital divide (Brodie et al., 2010; Hsu et al., 2005). In relation to E-health, the digital divide is a form of health disparity in healthcare's access to and use of both the information technologies and health information online (Brodie et al., 2000). Barriers to the emergence of an equitable information society have led to the existence of the digital divide (Liff & Shepherd, 2004). According to "Glocal" eHealth Policy context, developing countries trail far behind developed countries in E-health services and the widening gap has been attributed to several challenges: failure to develop E-health roadmaps by the Governments resulted from insufficient political will, lack of e-health experts or leaders to champion E-health projects, corruption, limited resources to finance the development of the project, poverty, frequent power outages, among others (Hogberg, 2005; Omary et al., 2009; Hellström, & Tröften, 2010; Kalogriopoulos et al., 2009).

2.5 Information and Communication Technology for Development (ICT4D)

Information and Communication Technology (ICT) refers to technologies that facilitate electronic means of creating, storing and disseminating information (Tiglao & Alampay, 2009). ICT includes 'old' ICTs such as radios, televisions and telephones, and 'new' ICTs such as personal computers, mobile phones and Internet (Raiti, 2007; Kleine & Unwin, 2009).

In recent years, there has been an interest in applying ICTs such as mobile phones for global development (Heeks, 2002). This is referred to as ICT for Development or ICT4D. It is relatively a new discipline that focuses on development issues presented by the World Bank initiative of 1995 (Chepken, 2012). It aims at bridging the digital divide by promoting equitable access of modern technology (Heeks, 2002; Pitula, Dysart-Gale & Radhakrishnan, 2010).

According to Mthoko and Pade-Khene (2013), many ICT projects fail to have a significant impact for intended users specifically in developing countries because such projects are implemented according to western techniques, and in isolation from the broader context of developing countries (McNamara, 2003; Sahlfeld, 2007; Ojo, 2007). Therefore, there is a need for technology research that is aimed at developing countries. ICT4D focuses on building technology artefacts for disadvantaged population based on user needs and requirements, and later on studying its impact on the community.

2.6 Information and Communication Technology for Healthcare (ICT4HC)

Information and Communication Technology for healthcare (ICT4HC) is a form of ICT4D. It refers to the use of ICTs to provide a reliable, timely, high quality and affordable healthcare and health information system (Chib, Lwin, Ang, Lin & Santoso, 2008).

Chib et al. (2008) proposed a model for ICT4HC based on the value-of-ICTs-to-education model (United Nations Development Programme, 2005). The model suggests that an ICT such as mobile phone can act as a producer of opportunity to increase the capacity and potential; enabler of social ties strengthen communication links within healthcare hierarchy, and with the patient to generate knowledge that would allow critical information to be shared and used effectively. Additionally, ICT4HC model addresses the presence of inter-related barriers that could hinder the translation of benefits into sustainable development goals. The obstacles of infrastructural factors were repeatedly noted in existing ICT4H model. However, Chib et al. (2008) noted that potential hurdles to ICT usage need to be explored further in order to provide a practical knowledge of ICTs in development.

2.7 International Standards and Regulations

According to Oppliger (1996), international standards can be defined as documented agreements containing precise criteria that must be followed consistently as rules, guidelines or definitions of characteristics to ensure that any products, materials, processes or services are fit for their purpose. The acceptance and adoption of these standards is recognized by very many states and governments in Europe, Asia, Canada, South America and some African countries (Tuyikeze, 2005; Tuyikeze & Pottas, 2005). Due to lack of standards and regulations specific to individual countries, Tuyikeze and Pottas (2005) from South Africa recommended that it is necessary to adopt other standards such as HIPPA, NIST or CCHIT certification to overcome some of the criticisms of ISO standards, such as being too general and therefore not providing stringent solutions to specific healthcare requirements. Therefore, we assembled eight evaluation criteria to represent legal requirements of the EHRs from NIST and CCHIT certification.

2.7.1 NIST Meaningful Use

The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS) is an agency in US that works with industries to develop and apply technology, measurements and standards. NIST provides certification programs to ensure that E-health systems offer the necessary functionality to help healthcare providers meet meaningful use criteria. NIST provides four criteria: the first criteria requires that users be given a unique name and/or identification number for tracking; the second criteria requires that controls should be established to permit only authorized users accessing patient's records; the third criteria requires that a user authorized for emergency situation be granted a set of privileges applicable only for emergency situation and lastly, the ability to activate emergency access roles.

2.7.2 Certification Commission for Health Information Technology (CCHIT)

The combination of NIST and CCHIT meaningful criteria are the driving force behind the implementation of access control in E-health systems. The goal of access control within E-health systems is to provide systems access control by ensuring that only authorized users have access to patient's information (Tuyikeze, 2005; Smith et al., 2010). In order to accomplish this goal, CCHIT provides four criteria: the first criteria requires that EHR systems must implement permissions such that users are only given least privilege; the second criteria requires administrative facilities to assign privileges to users and groups; the third criteria requires that EHR systems must implement either one of user-based access control (UBAC), context-based access control (CBAC) or role-based access control (RBAC); and lastly, EHR systems should allow a user to have their permissions removed without having to delete the user from the system. We use these criteria to analyse the systems we found in our literature search.

2.8 Study Approach

Below is the procedure followed for selection and inclusion of articles in the study.

i. A literature search was undertaken, based on the following keywords; electronic health record systems\tools\software, patient health record systems, electronic medical record systems, and personally controlled health record systems). Various databases were used to select our primary studies.

ii. We surveyed tools developed from 1999 to 2010 because it is during this time that EHR systems had gained much wider attention.

iii. The review excludes magazines, student's dissertations, newspapers and books among others. We were interested in analysing tools that are currently in use. Also excluded were tools and publications not written in English and studies without a sufficiently concrete description of implementation procedures. This means that the results may not be generalised to other E-health tools.

2.8.1 Selection Procedure

Initially, six online search databases were selected and a total of 157 EHR articles and systems were generated. Based on the titles, abstracts and procedures for the implementation of online health record systems, a total of 89 articles and tools were excluded. 68 articles met the selection criteria and were presented for further review. 44 articles were then excluded because despite having relevant titles, abstracts and full text, they did not present relevant tools for this study. The procedure for the selection of the articles is illustrated in Figure 2.1.

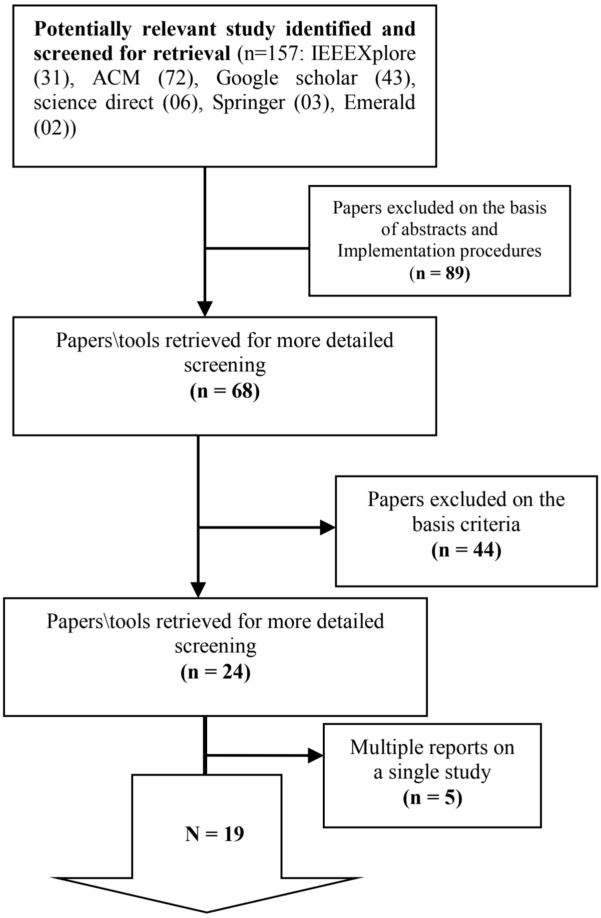

Potentially relevant study identified and screened for retrieval (n=157: IEEEXplore (31), ACM (72), Google scholar (43), science direct (06), Springer (03), Emerald (02))
Papers excluded on the basis of abstracts and Implementation procedures **(n = 89)**
Papers\tools retrieved for more detailed screening **(n = 68)**
Papers excluded on the basis criteria **(n = 44)**
Papers\tools retrieved for more detailed screening **(n = 24)**
Multiple reports on a single study **(n = 5)**
N = 19

Figure 2.1: Review flow diagram

2.8.2 Classification of Articles by Database

The majority of articles considered for this study were obtained from ACM and Google Scholar followed by IEEE. Science Direct and Springer had the least number of articles. Figure 2.2 gives the details. ACM and Google scholar maintained the highest number of articles because no restrictions of these databases at our institution and the two databases stores articles of various study fields including electronic health articles.

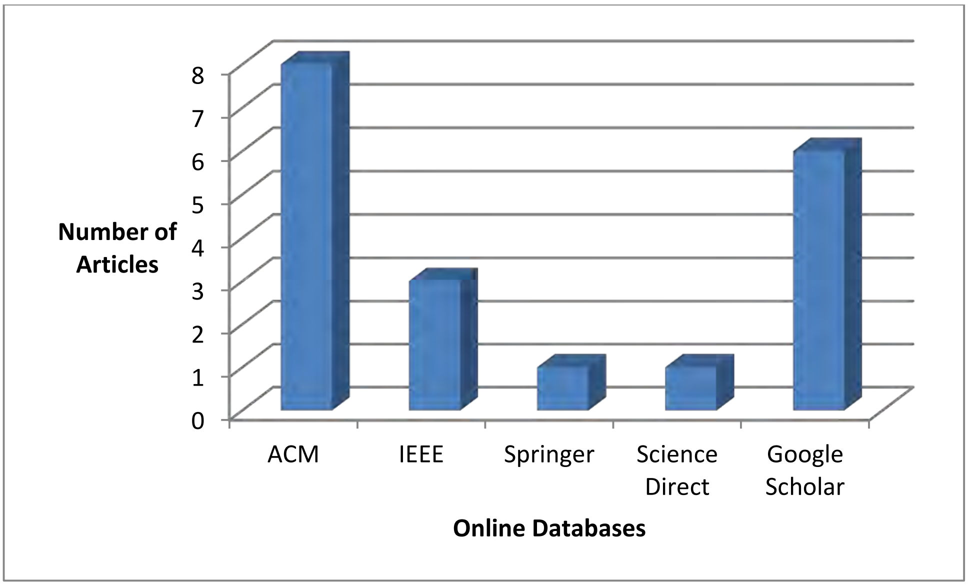


Figure 2.2: Number of Articles by Database

2.8.3 Classification by Year of Publication

Figure 2.3 shows the number of tools published per year in regard to our extraction. It is clearly indicated that from 1999 to 2004, there was a steady implementation of EHR systems. The number of publications increased from the year 2005 to 2008, with 2007 registering the highest number. From then on, there was a steady decrease in the number of publications with a decline in 2009 and 2010. This may be attributed to the fact that, some EHR systems were developed without proper understanding of the users and technology limitations and ended at demonstration stage. However, many published systems have been successfully implemented and used. Therefore, it makes sense to assume that the next healthcare generation will be characterized by access to EHRs for all.

2.9 Evaluation Criteria

In this section, we introduce the evaluation criteria, which offers an analysis of EHR systems based on three general dimensions i.e. technology, NIST meaningful use and CCHIT certification.

Technological features are sub-divided into development environments (DE), system platform and system type. System platform (Platform) classifies tools based on web/client-server platform (wp) or desktop platform (dp). Desktop platforms enable healthcare providers to record and store health information on a desktop based application.

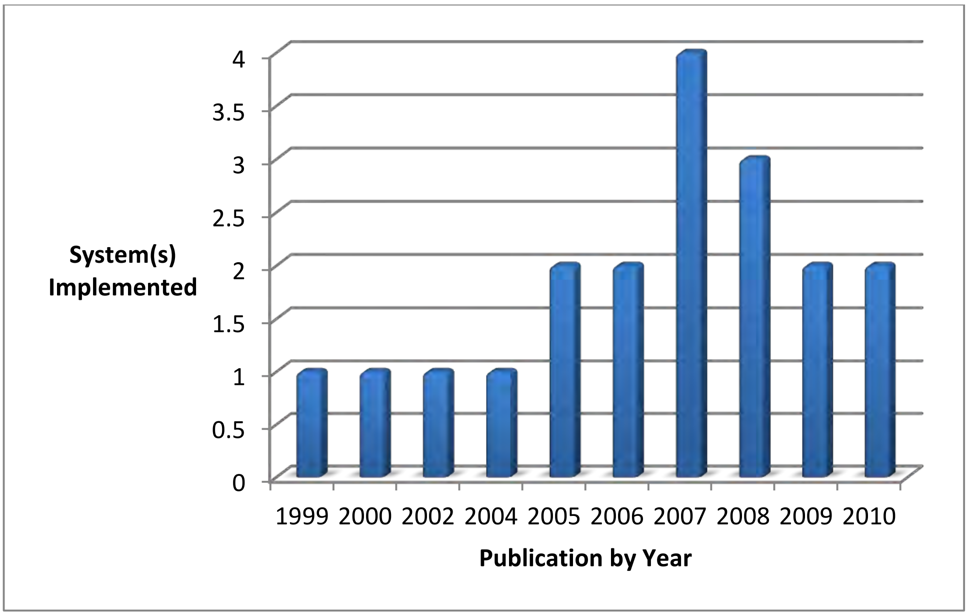


Figure 2.3: Number of Systems implemented per year

Client-server platforms use powerful servers with a high bandwidth connection to the network to hold centralized health information. System type (Type) classify tools based on whether they are meant to be purchased (p), have a complete free software downloadable version (dv) and/or meant for demonstration (d).

NIST meaningful use provides four criteria for our evaluation;

1. **NIST-U1:** Users given unique name and/or number.
2. **NIST-U2:** Access controls with defined user privileges.
3. **NIST-U3:** Emergency-time only privileges for user roles.
4. **NIST-U4:** The ability to activate emergency access roles.

CCHIT certification defines four criteria for our evaluation;

1. **CCHIT-M1:** Users are given least privilege permission set.
2. **CCHIT-M2:** Administrative facilities to assign privileges to users.
3. **CCHIT-M3:** Context-based access control (CBAC), user-based access control (UBAC), or role-based access control (RBAC).
4. **CCHIT-M4:** User role revocation without deleting a user.

Table 2.1 illustrates a classification of various EHR systems obtained from the review based on the dimensions described above.

Table 2-1: Summarized Classification Matrix Showing EHR Systems versus Dimensions

System/Dimension	Technology			NIST- Meaningful Use		CCHIT Criteria	
	DE	Platform	Type	NIST-U1, U2	NIST-U3, U4	CCHIT-M1, M2	CCHIT-M1, M2
HealthConnect	PerlOracle DB	wb	p	yes	no	Conf. dependant, yes	RBAC, Yes
Google Health	Java, .Net, XML, PHP, python	wb	dv	yes	no	Conf. dependant, yes	RBAC, Yes
Tool A	??	wb	d	yes	no	yes	RBAC, Yes
MEDIS	HTML, XML, JSP script language, Java? Apache & Tomcat web servers	wb	p	yes	no	Conf. dependant, yes	RBAC, Yes
Microsoft. HealthVault	.Net, Java, XML	wb	dv	yes	Conf. dependant, no	yes	RBAC, Yes
Indivo	Java, PHP, Tomcat, Apache Web Server 2.0, MySQL, PHP-Java Bridge 4.1.2	wb	dv	yes	Conf. dependant, no	yes	RBAC, Yes
FIS HealthManager	PIP, GT.M	wb	p	yes	no	Conf. dependant, yes	RBAC, Yes
VitalChart	??	wp	p	yes	Conf. dependant, no	Conf. dependant, yes	RBAC, Yes
OpenEMR	PHP, JavaScript, MySQL	wp	dv	yes	no	Conf. dependant, yes	RBAC, Yes
SmartPHR	XML??	wp	p	yes	no	yes	RBAC, Yes
Sharehealth	??	wp	p	yes	no	yes	RBAC, Yes
Dossia	XML, .Net (C#), Java, PHP	wp	dv	yes	Conf. dependant, no	yes	RBAC, Yes
iTrust	Java/MySQL, Apache Tomcat webserver	wp	dv	yes	no	yes	RBAC, Yes
WorldMedcard	PHP, .Net, Windows Server 2008, SQL server, ASP.Net, ISS,	wp	dv	yes	no	yes	RBAC, Yes
MyMedicalrecords.com	??	wp	p	yes	no	yes	RBAC, Yes
Tolven	J2EE framework, JBOSS application server, OpenLDAP	wp	dv	yes	no	Conf. dependant, need LDAP	RBAC, Yes
Myhealthfolders	.Net (aspx)	wp	dv	yes	no	yes	RBAC, Yes
Dr. I-Net	.Net (aspx)	wp	dv	yes	no	yes	RBAC, Yes
MediCompass	.Net (aspx)	wp	dv	yes	no	yes	RBAC, Yes

2.10 Discussion

In this section, we provide a description of 19 EHR systems analysed in Table 2.1 and summarize information about the applicability of these tools in developing countries. We also provide information on whether the systems passed or failed each of the 11 evaluation criteria presented in Section 2.7.

From the technological perspective, the biggest number of tools analysed are open source tools – those that have a complete free software downloadable version (Google Health, HealthVault, Indivo, Open EMR, iTrust, WorldMedcard, Tolven, Myhealthfolders, MediCompass and Dossia), followed by proprietary tools – those that are owned by companies and the source code is not accessible (HealthConnect, FIS' HealthManager, VitalChart, SmartPHR, Sharedhealth and Mymedicalrecords.com). The study further indicates that only one tool was designed for demonstration only (Mitamura et al., 2005). This therefore implies that the majority of tools in the matrix are open source tools. Dalle and Jullien (2002) argue that the openness of the source code is a key feature, which together with compatibility allows open source software to be advantageous over proprietary software. Increasingly, a vast number of proprietary tools do not mention their development environments and hence the use of "??" in the matrix.

Despite the flexibility proposed in the NIST and CCHIT certification in regard to access control, all the tools analysed used RBAC. Ferraiolo et al. (2001) highlighted that RBAC's flexibility provides the ability to simplify policy customization and make security policy management a non-technical job. The evaluation indicates that all the tools analysed are actively seeking to meet both NIST and CCHIT certification. All tools evaluated provide a set of pre-defined roles and permissions that an administrator can assign to users or groups of users. The pre-defined roles in the system represent a common role within the healthcare settings e.g. physician role, technician role etc. A user may be assigned one or more roles. Healthcare administrators have the ability to add any arbitrarily named role and assign it any number of privileges.

The evaluation further indicates that all tools met the first two NIST meaningful use criteria (NIST-U1 and NIST-U2), and only HealthVault, Indivo, VitalChart, and Dossia support emergency-time only privilege for user roles (NIST-U3). The lack of emergency access roles (NIST-U4) causes all the evaluated tools to fail to meet NIST meaningful use criteria. From the CCHIT certification, all the tools evaluated provide users with a given set of least privileges

(CCHIT-M1), enables the administrator to define roles for the users that guide information access in the system (CCHIT-M2) and also allows user revocation without first having to delete users from the systems (CCHIT-M4).

Daglish and Archer (2009) argue that patients need to be in control of their data such that those responsible for patients' care can perform their duties efficiently. Other reasons why patients need access to their health records include: records at the hospital server could be unreachable due to frequent power outages and/or unreliable Internet connections. Similarly, if the patient cannot give a new doctor access to his/her existing records, redundant tests may end up being used, resulting to different portions of patient's data being scattered among multiple EHRs. This makes it difficult for the doctors to have a complete picture of the patient's treatment history.

However, all tools in the matrix are designed for healthcare providers – patients have little or no access to their health records. Electronic health record systems such as Microsoft HealthVault, Indivo^{tm} and Dossia empower users with some access but the access must be online. In addition, all tools evaluated require online access control decisions. Solely relying on an online access control system is limiting, particularly in developing countries where access to the server is disrupted by a number of disastrous events. When the server becomes unavailable, for example due to power outages that is common in developing countries, access control decision cannot be made, making EHRs unreachable. Studies conducted by Sunyaev, Chornyi, Mauro and Kremar (2010), Daglish and Archer (2009), Baker and Masys (1999) highlights that any security mechanism needs to be usable; otherwise users will not use the system at all.

Furthermore, the infrastructure in developing countries is characterized by little or no Internet bandwidth, unreliable and intermittent main electricity and limited user expertise, among others (Omary et al., 2009; Mugwanya, 2013). This implies that developing countries require context relevant tools – tools developed with the unique constraints of the developing world in mind. However, all the tools explored are developed with user contexts in the developed world and thus do not represent the needs of the users in developing world. This can be witnessed by the existing manual paper based health records in most healthcare organizations in developing countries (Omary et al., 2009; Tierney et al., 2010; Kalogriopoulos, Baran, & Nimunkar, 2010).

Additionally, all the reviewed EHR systems assume some type of network connection as a basis for healthcare service provision: either through wireless or wired infrastructure.

Moreover, most of these systems have not been designed for mobile phone usage; rather, they were programmed for specific desktop platforms. Also, all the reviewed systems are based on the assumption that the end-user such as the patient initiates the search, browsing and download of personal health information (‘‘pull’’ model). Under no circumstances the delivery of information with no user intervention is enabled (‘‘push’’ model). One obvious disadvantage of the “pull” model is that the hospital is burdened with greater content management complexity. The hospital administrator needs to maintain outgoing records and keep them available until the intended receivers are willing to retrieve the records. Similarly, the hospital is burdened to ensure that the patients retrieving the records are indeed the originally intended the receiver.

2.11 Summary

Despite the potential of EHR systems to address the challenges facing health systems in developing countries, the majority of EHR systems designed for developed countries cannot be adapted for implementation in developing countries. The failure of adoption is attributed to many factors including;

1. **Online Access Control:** The majority of EHR systems require online access control decision. When the server/database is unavailable, for example due to frequent power outages that is common in developing countries, access control decisions cannot be made, making health records unreachable
2. **Users’ Context:** The majority of EHR systems designed for developed countries were developed with the user contexts in the developed World and therefore do not represent the needs of the patients and medical practitioners in the developing countries.
3. **Desktop Platforms Specific:** All the tools analysed were designed for desktop platforms, yet there are less than six computers per 1000 people in developing countries (Chinn & Fairlie, 2010).

We therefore consider that in order for EHR systems to satisfy the intended users specifically in developing countries, existing systems needs to be extended on mobile phones such that records can be made available when hospital servers are offline. Anokwa et al. (2012) affirmed that mobile phones (also called small handheld computers) can improve the provision of healthcare services in developing countries. The extended storage and processing capabilities are some of the design choices for millions of healthcare givers and patients in developing countries (Parikh & Lazowska, 2006)

2.12 Limitations

Although considerable attention was given to the classification framework design, some limitations still exist. First of all, finding the right key words for the database search was extremely difficult, and therefore some relevant articles might have been overlooked as much of the literature was selected based on a review of the title, keyword or abstract only. Secondly, the review was confined to papers that is in English language and could be accessed locally. Furthermore, due to restrictions on access of online search databases, the researcher only used university subscribed online databases, which were also restricted in some cases.

"The greatest danger in times of turbulence is not the turbulence;
it is to act with yesterday's logic."
- *Peter Drucker*

CHAPTER THREE: LITERATURE REVIEW

3. Introduction

This chapter offers a critical review of prior studies relevant to Personal Health Records (PHRs). Firstly, the chapter provides an overview of PHRs followed by PHR systems and lastly security models, which are the main research areas the thesis contributes. The related work on PHR is described under three general themes, namely: PHR systems models, legal and system standards, and security models with the goal of identifying and re-applying a security model that fits within the constraints of developing countries. Other subsections of this chapter identify key research gaps and explore the design and usability of interactive PHR technologies for patients. Based on the results, the chapter sets out a research agenda for the thesis, and justifies the selection of the security model that we used in our PHR system.

3.1 Patient Records

A patient record may be defined as any relevant record made by the healthcare professional from the time of consultation and/or examination to the application of health management (De Klerk, 1993). A patient record may contain information about the health of an individual, recorded by the healthcare professionals. The patient record documents the trend of medical activities over a particular period of time, including treatments, medications, prescription among others. There are at least two broad categories of medical records, namely: Electronic Health Records (EHR) and Personal Health Records (PHRs).

3.1.1 Electronic Health Records (EHRs)

An electronic health record is the electronic record of the medical information of a patient for a specific healthcare organisation, such as a hospital. EHRs have gained popularity in healthcare industry as an alternative to traditional paper-based health records. The basic concept of an EHR is to allow healthcare providers to store medically relevant data about a patient in the hospital database.

The EHRs can exist on standalone computers, networked server computers, removable disks or mobile devices and can be accessible online from interconnected network systems providing the opportunity for healthcare organizations to improve healthcare delivery (Haux, 2006). Electronic health records enable the efficient communication of medical information and thus reduce operating costs and administrative workload (Gunter & Terry, 2005). Other benefits of EHRs include; online lab test results, diagnoses, prescriptions, radiology reports, immunisation and medical histories (Garets & Davis, 2006; Robison, Bai, Mastrogiannis, Tan, & Wu, 2012). In general, EHRs offer the potential for better access to records when they are needed. Modern EHRs are accessed via stable Internet connections and support efficient sharing of health records among patients and healthcare providers (Garets & Davis, 2006). These modern EHRs are of great importance, since they have presented new possibilities for electronic health or E-health.

The major shortcoming of EHRs is the issue of data portability. An EHR can lose a great deal of utility if the patient chooses to change providers or moves to a remote area with no Internet connections. In cases where the patient has no access to his/her personal health record, it becomes impractical to export the data from the previous provider to the new provider (Robison et al., 2012; PCAST report, 2010).

3.1.2 Personal Health Records (PHRs)

A new development of Personal Health Records (PHRs) has evolved from EHRs. PHRs allow patients to add and annotate their own health records, which is typically not the case with EHRs. Unlike EHRs where providers control who adds or view patients' records, PHRs empower patients to become the custodians of their health records. Patients have full control of their health records.

There are two categories of PHRs. Paper-based PHR and electronic PHR. Paper-based PHRs are generally less portable between providers and in many cases, the cost of physically transporting the records is burdensome (Halamka, Mandl, & Tang, 2008). Additionally, according to the medical record standards, patient records should be kept for a certain number of years, and should be available at all times in order to support continuity of patient care (Carpenter, Ram, Croft, & Williams, 2007). Thus, keeping paper-based records for certain number of years incurs overwhelming storage costs.

Etzioni (2010) identified poor legibility as the major problem associated with paper-based PHRs, which in many cases results in serious medical errors. The interpretation of standard medical jargon and the standardisation of abbreviations are unreliable in paper-based PHR. Additionally, studies show that paper-based PHRs are disorganized, and they primarily focus on episodes, rather than continuum of patient care (Meidani, Sadoughi, Maleki, Tofighi, & Marani, 2012; Anokwa, 2010). The outcome is usually shortcomings in documentation in terms of accuracy, availability and legibility (Garrido, Jamieson, Zhou, Wiesenthal, & Liang, 2005; De Mul & Berg, 2007).

One way to overcome such shortcomings is to make use of Electronic Personal Health Records (EPHRs). EPHRs take the current paper-based records and convert them into a digital format. An EPHR is initiated by gathering health information of an individual from a single or multiple sources, such that information can be shared via the Internet with the authorised healthcare professional (s). The records include various types of data, such as physician's notes, medical conditions (diagnosis and treatment), medications (dose, frequency), laboratory and diagnostic test results (Kim & Johnson, 2002). Besides these, some PHR also provide insurance information, tele-medical events and genetic code map (Adida & Kohane, 2006; Sood et al., 2008).

Using EPHRs allows real-time access to healthcare records by both the patients and healthcare providers. Physicians, lab specialist, nurses, and patients can access the records via the Internet (Adesina et al., 2011). Additionally, EPHRs provide the opportunity to backup health information more easily than paper-based PHR records. This limits possible loss of healthcare records (Meingast, Roosta, & Sastry, 2006). Accessing EPHRs is easy because records are stored at the server, which runs an access control program to verify that the parties (health workers, insurance companies and other healthcare organization) accessing patient's records have appropriate permissions (Ssembatya, 2012). When a user makes a request to access the records, access control authorities verify the request and determine the access rights. A user with appropriate permission(s) is able to access the records. The process by which a user (patient) obtains his/her personal health records can be depicted in Figure 3.1.

Personal health records are accessed through personal devices such as a mobile phone via the Internet. The mobile phone-based PHR application interfaces to the hospital server to download the records onto the mobile device. The personal health records can also be continuously updated, irrespective of the location of the provider or patient. The ability to provide secure exchange of PHRs between providers and patients facilitates continuous access of health information and improve service delivery. Similarly, empowering patients to actively become involved in their healthcare and outcome provides many benefits to patients and healthcare providers. These benefits include: improving safety through better tracking of medications, improve the relationship between doctor and patient and generally improve the quality of care provided (Tang, Ash, Bates, Overhage, & Sands, 2006; Keselman et al., 2007; Detmer, Bloomrosen, Raymond, & Tang, 2008; Kaelber, Jha, Johnston, Middleton, & Bates, 2008).

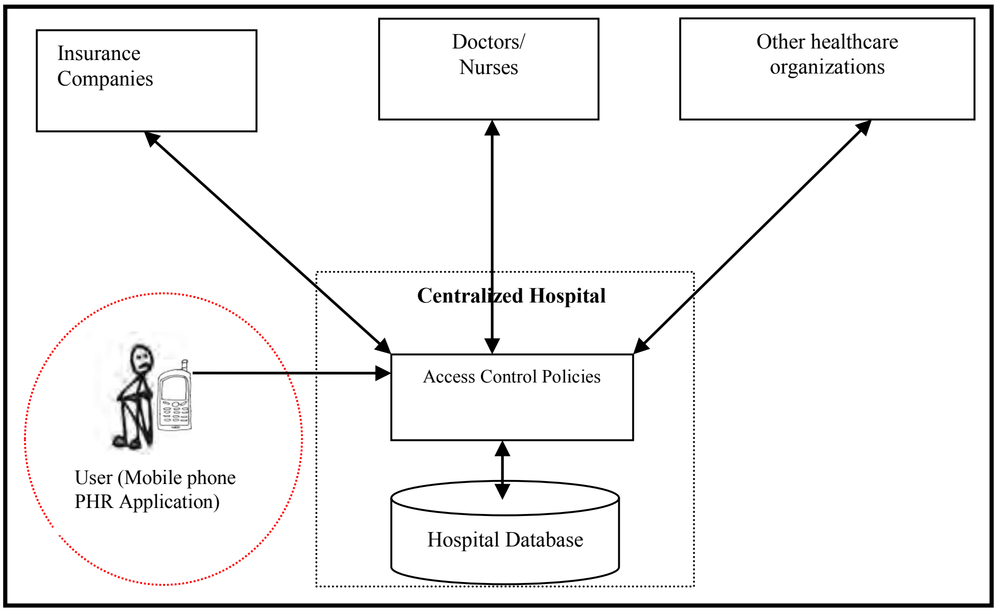


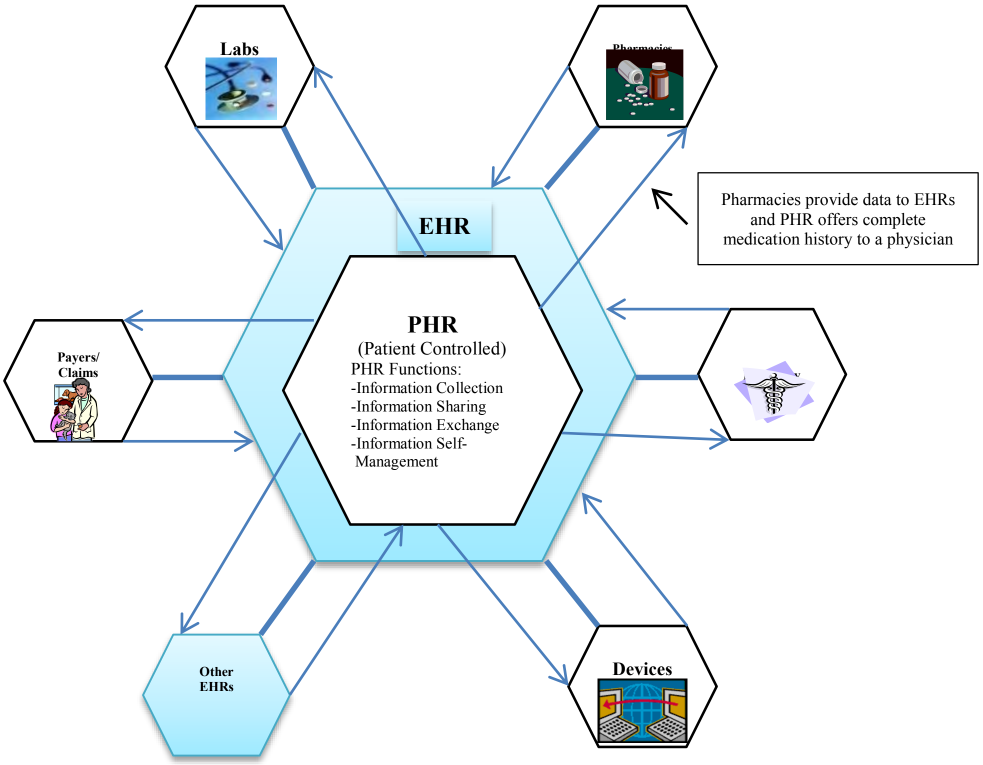
Figure 3.1: An E-Health Scenario showing PHR

As the case in conventional Internet-based EHR systems, access to PHRs is done via the Internet, which makes it vulnerable to unauthorised access. Additionally, eavesdropping and skimming can also occur when sensitive data are transmitted wirelessly (Garson & Adams, 2008; Adesina et al., 2011). With paper-based PHR, patients need to appear in person at the healthcare facility in order to receive treatment and medication, which restricts the number of personnel that have access to patient's information. Therefore, there is a greater challenge in ensuring security and integrity of PHRs compared to the traditional healthcare systems.

3.2 Definitions, Models and Context

One of the challenges of PHR research is to define a consistent description of what PHR actually entails. There is no generally agreed definition of PHR both in industry and government (NCVHS report, 2005). The Markle Foundation defines a PHR as a set of computer-based tools that enable users to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it (Markle Foundation, 2003; Kaelber et al., 2008). The definition of a PHR by the Markle Foundation has successfully predicted the evolving of PHR in the past ten years (Zheng, 2011).

According to Kaelber et al. (2008), the PHR and PHR system are described using a hub and spoke model, where a patient-controlled PHR is at the center connected to different stakeholders who exchange data and interact with patients (Figure 3.2). In this model, “the PHR becomes more valuable the bigger the hub (i.e., the more functions the PHR has), the more spokes it has (i.e., the more connected it is to other sources of health information), and the thicker the spokes are (i.e., the more complete the sources of health information are)”



Pharmacies provide data to EHRs and PHR offers complete medication history to a physician

Figure 3.2: The Hub and Spoke Model of the PHR System

The National Committee on Vital and Health Statistics (NCVHS) report (2005) outlined the attributes of a PHR system;

1. **Scope and Nature of Content.**
   All PHR systems have consumer health information such as medication, prescriptions allergies, laboratory results and chronic problems. Some PHR systems have information regarding immunisation.

2. **Source of Information.**
   The PHR data may come from the patient, caregiver, healthcare provider, payer, etc. Some PHRs may be populated with data from EHRs.
3. **Features and Functions.**
   PHR systems offer a wide variety of features, including among others: the ability to view personal health data, exchange secure records with providers, ability to transfer data to or from an electronic health record, schedule appointments, renew prescriptions and enter personal health data; decision support: such as medication interaction alerts or reminders about needed preventive services and the ability to track and manage health plan benefits and services.
4. **Data Storage.**
   The data (health records) may be stored in a variety of locations, including: centralised database, accessed through the Internet, a provider's EHR, the consumer’s home computer, a portable device such as a mobile phone, or a database privately owned by the consumer.
5. **Custodian of the Record.**
   The PHR record may be operated by a number of stakeholders, including the patient, a healthcare provider, an independent third party, an insurance company or an employer.
6. **Party Controlling Access to the Data.**
   In many cases, consumers/patients must have exclusive control of their records.

Based on the attributes identified by NCVHS, we give another definition of PHRs and PHR systems: “PHR refers to electronic, universally available personal health information, obtained from a single, or multiple sources of EHR systems in a secure and confidential environment. PHR systems refer to the computerised tool that enables patient-users to comprehend and manage their health information stored in a PHR”. Thus, PHR systems allow patient-users to securely access and maintain their personal health information in order to support quality healthcare.

3.3 PHR Functions

The functions of a patient controlled PHR fall into four general categories;

1. **Information Collection**
   This function enables patients to securely retrieve their personal health information from external sources.

2. **Information Sharing**

   This PHR function allows patients to engage in one-way sharing of their health information with authorised stakeholders.

3. **Information Exchange**

   The information exchange function allows patients to engage in two-way information exchange with other stakeholders.

4. **Information Self-Management**

   This PHR function allows patients to better manage their own health or healthcare. Examples of PHR functions in this category include those functions that allow patients to record and track health information about their own health, as well as obtain relevant patient oriented disease information and decision support.

Based on the four PHR functions, one can reason that PHRs can improve the patient-provider relationship and enhance patient decision making. Table 3.1 below summaries other potential benefits of PHRs from the perceptive of various roles.

Table 3-1: Potential Benefits of PHRs and PHR systems

Roles	Benefits
Healthcare Providers	✓ Improve access to data from the patients ✓ Avoid duplicate testes ✓ Improve medication compliance ✓ Improve documentation of communication between healthcare providers, caregivers and patients ✓ Increase knowledge of potential drugs and persistent allergies ✓ Provide patients with convenient access to specific information such as lab results
Patients and Caregivers	✓ Promote portability of personal health information across providers ✓ Supports timely access to information ✓ Avoid duplicate testes ✓ Supports healthcare decisions and responsibility for care ✓ Support understanding and appropriate use of medication ✓ Improve understanding of health issues ✓ Verify and alert the provider about the inaccuracy of information

	✓ Strengthen communication with the providers ✓ Improve documentation of communication with patients ✓ Support wellness activities ✓ Increase sense of control over health ✓ Increase control over access to personal health information ✓ Support continuity of care across providers ✓ Reduce adverse drug interactions and allergic reactions
Employers	✓ Provide convenient service ✓ Use aggregate data to manage employee's health ✓ Support preventive care ✓ Promote empowered healthcare consumers ✓ Improve productivity of the staff
Payers	✓ Provide information and education to the beneficiaries ✓ Improve customer service ✓ Support wellness and preventive care ✓ Promote portability of patient information across plan
Population Health Benefits	✓ Strengthen health promotion and disease prevention ✓ Expand health education opportunities ✓ Improve the health of populations

3.4 Optimal characteristics of PHRs

Recently, a number of PHRs have begun to provide patients with secure access to manage their health information. However, the literature reveals that there is no standard framework for a PHR (Sood et al., 2008). Tang and Lansky (2005) identified five key characteristics of an optimal PHR.

First, a PHR should include a lifelong comprehensive patient record. In order to be a lifelong record, both the design and technical standards used in the development must support information exchange and portability. In the earlier model (the hub and spoke model of the PHR system), it is often up to patients to consolidate their records from various EHR systems in order to support information exchange and portability. Secondly, a PHR should support immediate accessibility of the patient information as needed. This is particularly important during emergency situations that require immediate access of patient's medical history. Thirdly, the PHR must provide health management and information tools that assist patients to understand the information contained in their record, together with recommendations for improving their health. Fourth, the PHR system must provide functions that guarantee patient's privacy and security of their health records. In addition, the PHR system must be transparent in terms of information access and information sources (Sood et al., 2008). Lastly, patients must have control of who has access to the information contained in their PHR.

3.5 PHR Models

Several PHR models are evolving, which vary in who manages and controls the health information. In this section, we present the four different PHR models and describe the characteristics of each model.

3.5.1 Provider-Based PHR Model

There are several options of this type of PHR, but they all share the following characteristics:

- The personal health record is read-only for the patients, enabling the providers to supply, control and maintain the record.
- Patients are only permitted to view their personal health information and schedule appointments.

Some hospitals permit patients to see a limited set of information, such as lab test results or radiology interpretations, assembled from their electronic data stores. These are typically made available to the patient from a password-protected Web-based system. Some commercial electronic health records (EHRs) are starting to offer the same sort of digital summary through patient portals and are calling this a PHR (Endsley, 2006).

Under this model, health information generally is tethered to the provider, who manages and controls the patients' ability to collect and synthesize information. Bernstein et al. (2008) acknowledged that the provider-based PHR model is a simple model that can act as a starting point for the more sophisticated models.

3.5.2 Health Plan or Employer-Based PHR Model

In this type of model, employees can access their claims data and benefit information via a portal hosted by an independent outsourcing partner or employer. Users can receive wellness education and enter their medical histories and other information. Similar to the Provider-based PHR model, Employer-based PHR model is also tethered on one source – the health plan or employer. Consumers get claims from multiple healthcare providers because all the claims are paid by the same payer. However, they cannot access content-rich clinical information, because each clinician controls the health records in his or her possessions. In addition, a health plan creates the capacity to generate and store claims data and clinical information that both the providers and patients can generate, including information about lab results and medications.

The funding for employer-based personal health records is based on reducing total healthcare costs to the employer through wellness and coordination of care (Bernstein et al., 2008).

3.5.3 Vendor-Supplied PHR

Another common case of the PHR model is the Vendor-supplied PHR model. In this model, a vendor offers a product, which serves as a secure container for patients to retrieve, store and manipulate their personal health records. Examples of vendor-supplied PHR include Microsoft's HealthVault, which empower users to upload and store their personal health records at HealthVault server. The business model for Vendor-supplied PHR is generally based on attracting more users to advertise on their website, targeting users of the free PHR service.

3.5.4 Patient-Centric PHR model

In the patient-centric PHR model, patients control their entire PHR via web portals or portable computing devices such as mobile phones in order to import, read and update their records. This model increasingly allows compatible devices to upload personal health records directly to patient PHR via appropriate interfaces. The majority of patient-centric PHR systems are Internet-based products. As with many other types of PHR models, a patient-centric PHR system consists of three primary components: the data, infrastructure and applications.

Data are the types and elements of information that are analysed, stored and exchanged by different information technologies. Examples of data include medication history, laboratory and imaging results, healthcare claims information, and lists of patients' medical problems. Infrastructure is the computing platform(s) such as software package(s), functions or websites, which exchange and process healthcare data. Applications are the capabilities and outputs of health information systems themselves, and are enabled through data and infrastructure (Kaelber et al., 2008).

Applications include data exchange and transactional capabilities such as medication renewals, analytical capabilities such as patient decision support, and content delivery capabilities such as disease education contents. All the three components are critical for effective PHR systems. The PHR functions exist in the PHR infrastructure and applications, and process data used in the PHR.

PHR specialists develop patient-owned software programs that empower individuals to organise and retrieve their own health information. The PHR software can reside on a personal computing device such as mobile phone or can be a web-based. In the earlier case, the health data and the screen interfaces for retrieving the data are maintained by the PHR owner (Kaelber et al., 2008).

3.6 The Hub and Spoke PHR Model

The four emerging PHR systems can be derived from the hub and spoke model (Kaelber et al., 2008). For example, the provider-based PHR system can be considered in the hub and spoke model with just one thick spoke, where provider-based PHR system is tied to the healthcare organisation's internal record system. The benefits of the different PHR systems and how a complete hub and spoke PHR system would be developed vary depending on how specific patients receive care (Kaelber et al., 2008). Zheng (2011) considered interoperability of a PHR system as a full version of the hub and spoke model. If PHRs are to be viewed as data repositories of patient's data (Figure 3.2), then interoperability (in terms of importing and exporting information from a PHR) is critical. Löhr, Sadeghi and Winandy (2010) acknowledged that, advanced PHR system will function as seamlessly integrated and/or interoperable subsystem of other health systems in the future.

3.7 PHR Infrastructures

A PHR system can be built upon various types of infrastructure such as, personal computers, portable devices (mobile phone and USB), the Internet, and can also be a platform-based PHR (Robison et al., 2012). In the next section, we describe the three types of PHR, built on portable devices (device-based PHR), the Internet (Internet-based PHR) and platform specific (Platform Style PHRs)

3.7.1 Device-Based Personal Health Records (PHR)

As noted earlier, the issue of data portability is one of the major shortcomings of EHRs, particularly in developing countries. One promising type of PHR that can address the portability problem is the device-based PHR that can easily be carried by the patient from one location to another. A device-based PHR typically consist of a mobile device such as a mobile phone, preloaded with some software intended to download and organise health information on the mobile phone. It gives patients considerable control over their health records, and provides much greater opportunity for portability (Robison et al., 2012). The device-based PHR typically provides functionalities for automatically interfacing and synchronising with the hospital server in order to provide up-to date health records (Robison et al., 2012). This makes a mobile phone-based PHR more valuable in healthcare delivery. Isolated PHR systems of this nature are built on the patient-centred model, which establishes a partnership among healthcare providers, patients, and their families (when appropriate) and ensures that, decisions made by healthcare professionals respect patients' needs and preferences (IOM report, 2001).

Due to their offline nature, mobile phone-based PHRs can provide patients with a mechanism to communicate with their providers when the hospital servers are offline (Avancha et al., 2012). Because a mobile phone-based PHR can easily be extended, it gives the opportunity to integrate other tools such as decision support tools and can also make use of medical sensors (Gay & Leijdekkers, 2007). However, as in EHR systems, a mobile phone-based PHR also raises questions pertaining to security and privacy (Zheng, 2011; Avancha et al., 2012).

3.7.2 Platform Style PHRs

Platform-based PHR system provides a repository for the patient's health data, and allows the health data to be shared and manipulated by any platform-supported PHR apps that are selected by the user (Robison et al., 2012). The PHR apps provide a range of functionalities including: functions to assist patients to maintain their health records, by importing data from external sources, or provide a user friendly interface for manual input of the data, keep tract of the medications taken, provides medical history of the patient or help the patient visualise and understand laboratory results (Mandl et al., 2012).

Figure 3.3 shows a simplified flow of how PHR apps interact with the PHR system and the users. In this diagram, the patient is using an app to view his/her personal health records while the physician is using an entirely different app to enter/view patient's records in/from the EHR system. The upload function adds health data recorded by the healthcare professional to the PHR automatically.

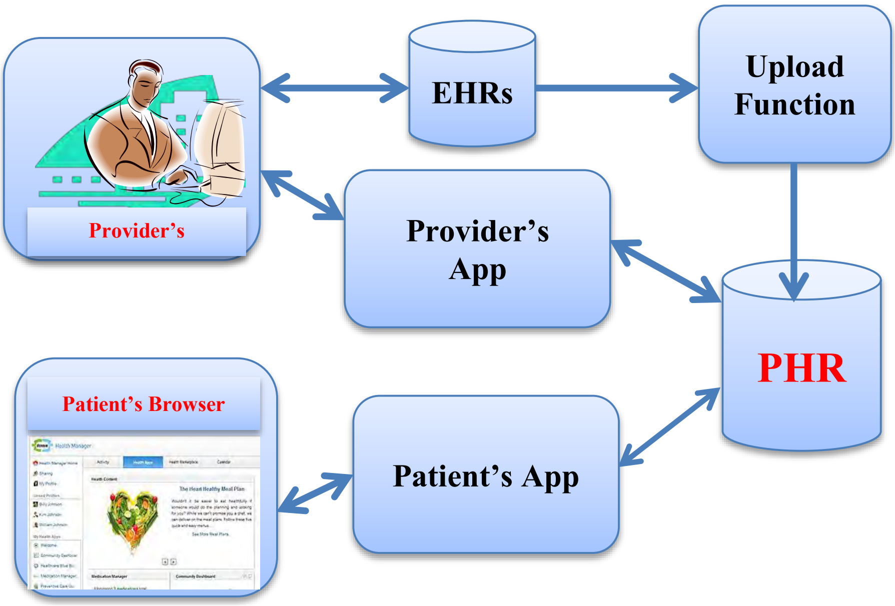


Figure 3.3: Simplified Platform Style PHR Flow

3.7.3 Internet-Based Personal Health Records (PHR)

Internet-based, personal health records have widely influenced the delivery of healthcare services in the 21st century. It includes any Internet-accessible health application that enables patients or their families (when appropriate) to create, review, annotate or maintain a record of any aspect of their health conditions such as medical problems, allergies and/or vaccination history (Sittig, 2002). Internet-based PHRs have shown greater potential than standalone systems in that, they provide better opportunities to change the way health data is used (Robison et al., 2012). With standalone PHR systems, there is a danger of each system to contain only a subset of the record, which greatly limits its value (Tang et al., 2006). Internet-based PHR gives the healthcare provider the possibility to contribute to the medical records directly, such that PHR systems can automatically import the data from the provider's EHR system (Win et al., 2006; Robison et al., 2012).

3.8 PHR Studies Discussion

There are a number of interesting findings that have been presented in this section. First, relying on paper-based PHR systems in healthcare organisation such as a hospital impose many disadvantages ranging from incorrect recording of diagnoses to exclusion of patients from accessing their health records. Patients need to be the custodian of their health records in order to be involved in the delivery of care (Weitzman, Kaci, & Mandl, 2009). Secondly, based on our literature review, most previous PHR studies focused on the areas of information self-management and information exchange. In these areas, PHRs have the potential to dramatically improve the patient-provider relationship and enhance quality healthcare. Similarly, literature has revealed that majority of healthcare providers in developed countries have adopted Internet-based PHR systems and found them useful in terms of patient empowerment. Empowering patients to own their health records motivates them to use and keep the records updated, which in turn makes it more valuable to the healthcare providers (Robison et al., 2012).

As third party developers produce more PHR applications, researchers have predicted that more users including those in developing countries will take advantage of PHR systems in order to add value to their personal health records. Therefore, the expressed focus of this thesis is to investigate the usefulness of PHR systems in developing countries despite the usual problems of poor infrastructure and illiteracy level.

Additionally, although majority of studies have presented different opinions regarding how PHR systems should be implemented, privacy and security of patients' health record appeared to be the most common concern of all studies. Confidentiality of patient's health records should not be overlooked when designing a PHR system (Win et al., 2006).

In the next section, we present a survey of legal and system standards for healthcare information technology (IT). The section describes some of the existing laws and policies related to PHR management and exchange.

3.9 Survey of Privacy Laws and Regulations

The United Nations general assembly adopted a set of guidelines on privacy and data protection in solution 45/95 of 1990 (UN guidelines, 1990). The guidelines encourage countries to enact legislation that will accord personal information an appropriate measure of protection. It further ensures that such information is collected only for appropriate purposes and by appropriate means. In 1995, the Data Protection Directive was enacted to provide some level of protection for citizens during the free flow of personal data within the European Union (EU).

The National Health Service (NHS) in the UK has developed a national scale system of electronic health records basing its privacy practices on the EU Data Protection Directive: data purpose specification, openness, individual participation, collection limitation, data quality, use limitation, data security safeguards, and accountability (NHS, 2009). Generally, these conditions fall into three major categories: (1) Informed user consent, (2) Legitimate purpose and, (3) Relevancy and purpose of the data collected. Furthermore, the EU Data Protection

Directive states that, personal data can be transferred to another country outside EU only if that country offers adequate level of protection (EU, 2009).

Based on the EU directive, most countries have developed broad data protection and privacy laws. These laws cover a range of personally identifiable data including health-related information. The laws deal with privacy aspects such as legitimacy of need-to-know, notification, consent, individual’s rights with respect to access, examination and amendment of data, and requirements for security safeguards. The laws further provide remedies and sanctions against violations. The majority of the laws are administered through independent national data protection commissions (Avancha et al., 2012).

3.9.1 The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress, and signed by President Bill Clinton to help improve healthcare delivery (HIPAA, 2010). The act “specifies the privacy, security and electronic transaction standards with regard to patient information for all health care providers” (Volonino & Robinson, 2004). HIPAA regulates healthcare providers such as hospitals on the permissible use and disclosure of identifiable health records (Kulynych & Korn, 2003). It involves two major provisions; insurance reform, so that pre-existing medical conditions do not lead to refusal of coverage when a person changes location, and simplifying administrative tasks, intended to reduce healthcare costs by standardizing information transactions (Mercuri, 2004). HIPAA seeks to validate the unavoidability of electronic data transactions in order to address privacy and security issues of electronic transactions (Choi, Capitan, Krause, & Streeper, 2006). The Privacy Rule protects personal health information by dictating how and when personal information may be disclosed and for what reasons. It encourages more involvement of patients, by giving them specific rights to access their health records and restrict the disclosure of their health information (Choi et al., 2006).

The security rules requires compliance actions in the following categories;

1. **Administrative safeguards**: The formal practices for security management and personnel
2. **Physical safeguards**: Concern about protecting EHR systems and the facilities within which they reside

3. **Technical safeguards**: Provide means to control and monitor information access, including technology to secure data-in-transit
4. **Organizational requirement**: Deals with business associate contracts
5. **Policies, procedures and documentation requirements**: Similar to those in Privacy Rules

Generally, HIPAA Security rule defines three requirements for access control (HHS Security standards, 2003);

1. **HIPAA-H1:** Unique identifier for each user
2. **HIPAA-H2:** Generalized access control for users
3. **HIPAA-H3:** Emergency access procedures

The emergency access procedures should enable healthcare professionals to access patient's information under abnormal circumstances. For example, if EHR system operations have been damaged, there must be an access control procedure that enables individual-users such as patient or clinical officer to gain access to the needed electronic health information.

3.9.2 Privacy Laws and Regulations outside EU

A number of countries have developed data protection and privacy laws. For example, the 1993 Privacy Act of New Zealand was one of the most comprehensive Privacy Act outside European Union (NZPA, 1993). The act applies to personal information collected by businesses and governmental agencies. It covers twelve principles based on the Organization for Economic Cooperation and Development (OECD) privacy guidelines and the National Information Principles contained in the Australian Privacy Act. Other principles in the Act that are not part of OECD include: data collectors should specify the manner of collection, agencies should not keep information longer than necessary, and information should be checked for correctness before use (NZPA, 1993).

In Africa, countries such as Angola, Burkina Faso, Tunisia, Morocco and Senegal have adopted privacy legislation (Makulilo, 2012), whereas, countries in Sub-Saharan Africa such as Uganda, Rwanda and Tanzania are still in the process of drafting privacy laws. Other countries such as Ghana, Ivory Coast, Kenya and Mali have their bills on similar law pending before their legislative bodies (Makulilo, 2012). Therefore, it is imperative to mention that this development is largely due to the inertia of the European Data Protection Directive.

3.10 Laws and PHR Discussion

While the laws and regulations described above outline the legal protection for PHR privacy and security, they don't address all the issues involved in the PHR system. Precisely, the majority of the laws and regulations described above apply to "covered entities" including health plans, healthcare clearing houses and healthcare providers (Kaelber et al., 2008). PHR systems should protect a patient's privacy and security even outside the covered entities. In contrast, the laws and regulations in the EU Directive 95/46/EC apply to personally identifiable data regardless of the settings. This therefore means that the EU Directive applies to PHR and all the practices of PHR technologies.

3.11 The International Health System Standards

A number of standards have been developed by the healthcare industry, through which health records can be transferred among different healthcare systems. These standards include and are not limited to Health Language Seven (HL7), Health Insurance Portability and Accountability (HIPAA), Continuity of Care Record (CCR) and Continuity of Care Document (CCD). In order to design a PHR system that offers high interoperability, there is a need to assess the PHR standards. Current PHR systems usually support multiple healthcare information standards, which makes it possible to interoperate with other systems and provide standardized interface between different healthcare systems.

3.11.1 The Health Level Seven International

The Health Level Seven International (HL7) is the global authority on standards for interoperability of health information technology. It was founded by a group of healthcare computer system users who started developing the HL7 protocol to allow sharing of clinical data with each other, and has since then become the global standard (HL7 Standard). The mission of HL7 is to:

> "*Provides standards for interoperability that improve care delivery, optimize workflow, reduce ambiguity and enhance knowledge transfer among all of our stakeholders, including healthcare providers, government agencies, the vendor community, fellow SDOs and patients. In all of our processes we exhibit timeliness, scientific rigor and technical expertise without compromising transparency, accountability, practicality, or our willingness to put the needs of our stakeholders first"* (HL7 Standards).

These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between healthcare systems. HL7 standards support clinical practice and the management, delivery, and evaluation of health services, and are recognized as the most commonly used in the world (HL7 Standards).

The major purpose of HL7 standard is to facilitate improvements in five main areas:

1. Interoperability
2. Safety/security
3. Quality/reliability
4. Efficiency/effectiveness
5. Communication (i.e. verbal and written communication to improve understandability)

From the healthcare perspective, all these are clearly important to improve quality healthcare. However, interoperability is arguably the single most important benefit among others, since without interoperability; the ability to achieve the other three benefits is significantly limited (Dickinson, Fischetti & Heard, 2004).

Hl7 demonstrates that, healthcare systems must be compatible to each other in order to allow standard-based communication among various kinds of healthcare applications (Dudeck, 1998). A validation mechanism to verify the data consistency is needed. Some EHR systems provide validation services for various standards such as the HTML validation service in W3C[10]. Recently, extensible mark-up language (XML) has become the standard format for data exchange between EHR applications on the Internet (HL7 Standards). Exchanged information is distributed in XML format and uses document type definition (DTD) to specify data structures and grammar to allow different systems to know each other (Morrison et al., 2000). XML has proved to be a valuable document structure for electronic data exchange in the medical field and other different settings (Wolff et al., 2001; Rassinoux, Lovis, Baud, & Geissbuhler, 2003; Müller, Ückert, Bürkle, & Prokosch, 2005).

HL7 is an open system standard whose interface allows for numerous systems to be added to a single feed (HL7 Standard). It provides a mechanism by which users can interact with multiple

[10] http://validator.w3.org

reporting systems regardless of the platforms. Figure 3.4 below illustrates HL7 interface model, which allows users to interface with multiple systems regardless of the implementation platform.

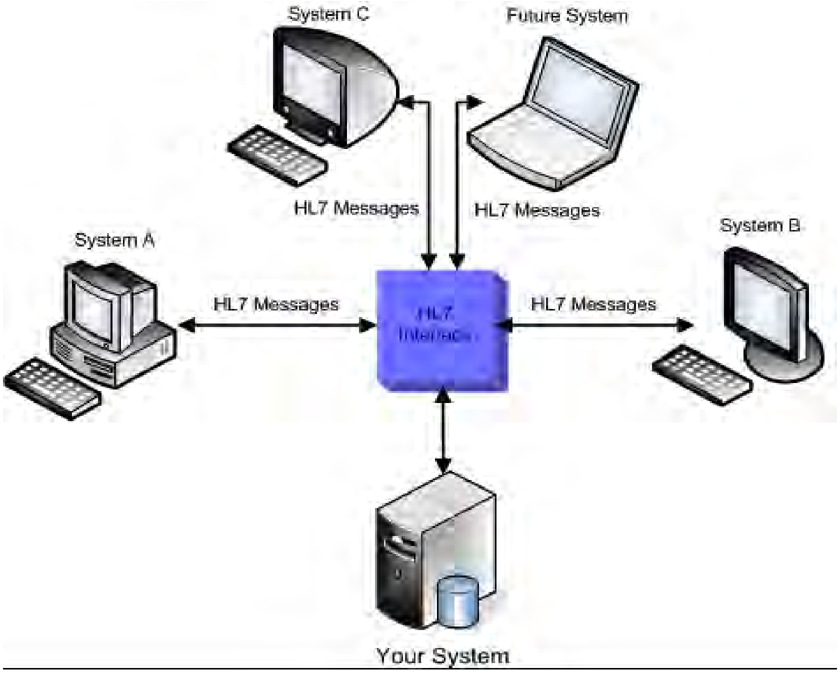


Figure 3.4: HL7 Interface Model (INTERFACEWARE, 2008)

3.11.2 The Continuity of Care Record (CCR)

The Continuity of Care Record (CCR) is a core data set of the most clinical information about a patient. It provides a means by which healthcare providers aggregate health data about a patient and forward it to another provider or patient in order to support the continuity of care (ASTM International, 2009). The CCR was developed jointly by ASTM International, the Massachusetts Medical Society (MMS), the Health Information Management and Systems Society (HIMSS), and the American Academy of Family Physicians (AAFP). Its goal is to improve continuity of patient care, reduce medical errors, and to assure minimum standard of health information transportability. The Standard Specification for Continuity of Care Record states that;

"The CCR document instance must be self-protecting when possible, and carry sufficient data embedded in the document instance to permit access decisions to be made based upon confidentiality constraints or limitations specific to that instance" (ASTM International, 2009)

The conditions of security and privacy for the CCR instance are established in a way that allows only properly authenticated and authorized access. The CCR consists of three core components:

the CCR Header, the CCR Body, and the CCR Footer. Figure 3.5 below presents the conceptual model of the CCR, showing the three core elements on the left and potential extensions on the right.

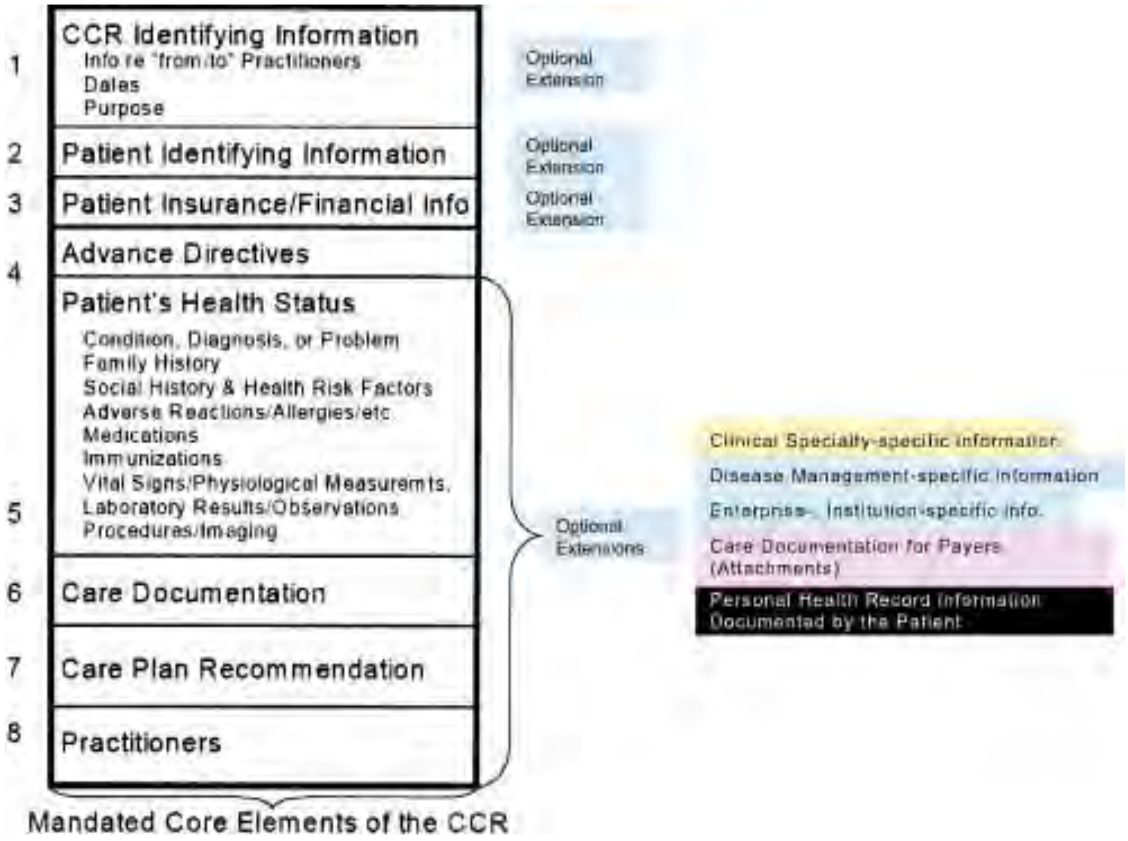

1
CCR Identifying Information
Info re "from/to" Practitioners
Dates
Purpose
Optional Extension
2
Patient Identifying Information
Optional Extension
3
Patient Insurance/Financial Info
Optional Extension
4
Advance Directives
Patient's Health Status
Condition, Diagnosis, or Problem
Family History
Social History & Health Risk Factors
Adverse Reactions/Allergies/etc
Medications
Immunizations
Vital Signs/Physiological Measuremts.
Laboratory Results/Observations
Procedures/Imaging
5
Optional Extensions
Clinical Specialty-specific information
Disease Management-specific information
Enterprise-, Institution-specific info.
Care Documentation for Payers (Attachments)
Personal Health Record Information Documented by the Patient
6
Care Documentation
7
Care Plan Recommendation
8
Practitioners
Mandated Core Elements of the CCR

Figure 3.5: Conceptual model of Continuity of Care Record (The ASTM E31.28, [Accessed 16/05/2013])

The aim of CCR is to provide healthcare professionals with all the relevant information needed for patient’s care. In relation to an EHR, the CCR have been described as the data extract (Ferranti, Musser, Kawamoto, & Hammond, (2006). As highlighted in the implementation guide, ‘‘the CCR represents the patient summary, which for many EHRs is called the ‘overview’ of the patient.’’(Tessier, 2004). In principle, the CCR extracts relevant information from various health documents and creates a “snapshot” of the patient. Figure 3.6 describes the idea of CCR standard. The CCR pools health information from EHR to enable the exchange of electronic health records among care providers and between providers and patients.

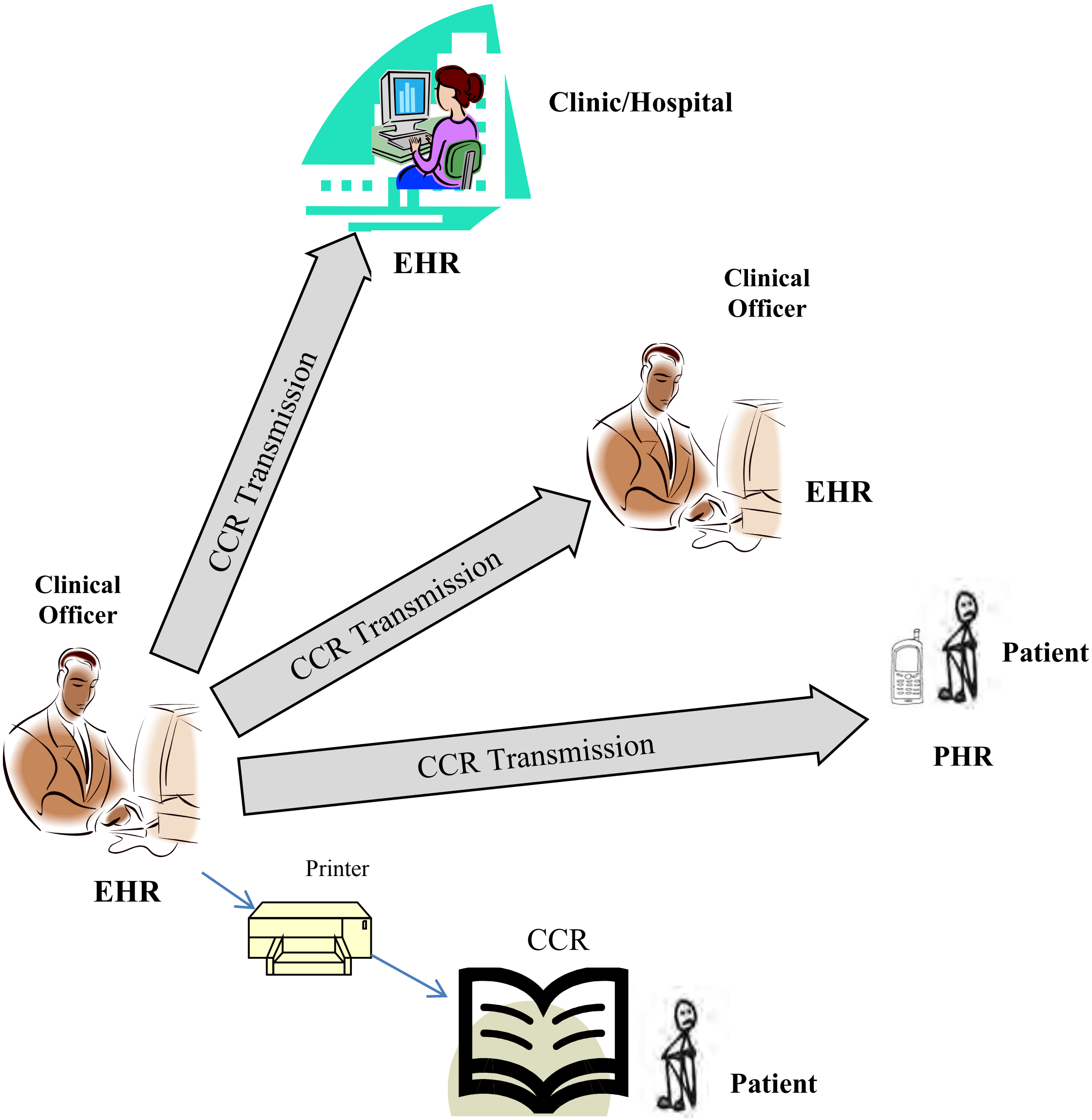


Figure 3.6: The idea of CCR standard

3.11.3 The Clinical Document Architecture (CDA)

In contrast, CDA is based on a formal information model and can be used for a number of document types, including clinical summaries, progress notes and discharge summaries (Ferranti et al., 2006). CDA is based on the principle of incremental interoperability, where the healthcare provider can begin with a simple CDA and then add structured data elements over time (Dolin et al., 2001). A CDA document contains a header and a body. The header carries identification and administrative information for the document.

The body contains statements that make up the actual content of the document. The header makes it possible to exchange “clinical document”[11] across and within institution and facilitates the compilation of patient’s records into a lifetime EHR.

According to Dolin et al (2001), the CDA header has four main components;

1. **The document information:** The document information identifies the document, defines the confidentiality of the document, and describes its relationships with other documents.
2. **Encounter Data:** This component describes the setting through which the documented encounter occurred.
3. **Service Actors:** This component includes those who authenticate the document, the intended receiver of the document, document originators and transcriptionists, and healthcare providers who participated in the documentation.
4. **Service targets**: This includes the patient and other participants (such as family members) that can have access to individual’s health records.

Both the Clinical Document Architecture (CDA) and the Continuity of Care Record (CCR) strive to facilitate the interchange of health care data among healthcare providers (Ferranti et al., 2006). Furthermore, they both use the World Wide Web Consortium standard of Extensible Mark-up Language (XML) to facilitate the exchange of structured health data (WWW Consortium, 2008). Similarly, because CDA and CCR are both XML standard documents, they are be both machine and human readable, and the data content may be displayed or printed in a variety of formats, including the web browser, PDF reader and/or word processor (Ferranti et al., 2006). Figure 3.7 shows a CCR/CDA file describing a “snap shot” of a patient’s health history that can be created from a single or multiple sources of EHRs, PHRs and health plans.

[11] A clinical document is a documentation of clinical observations and services

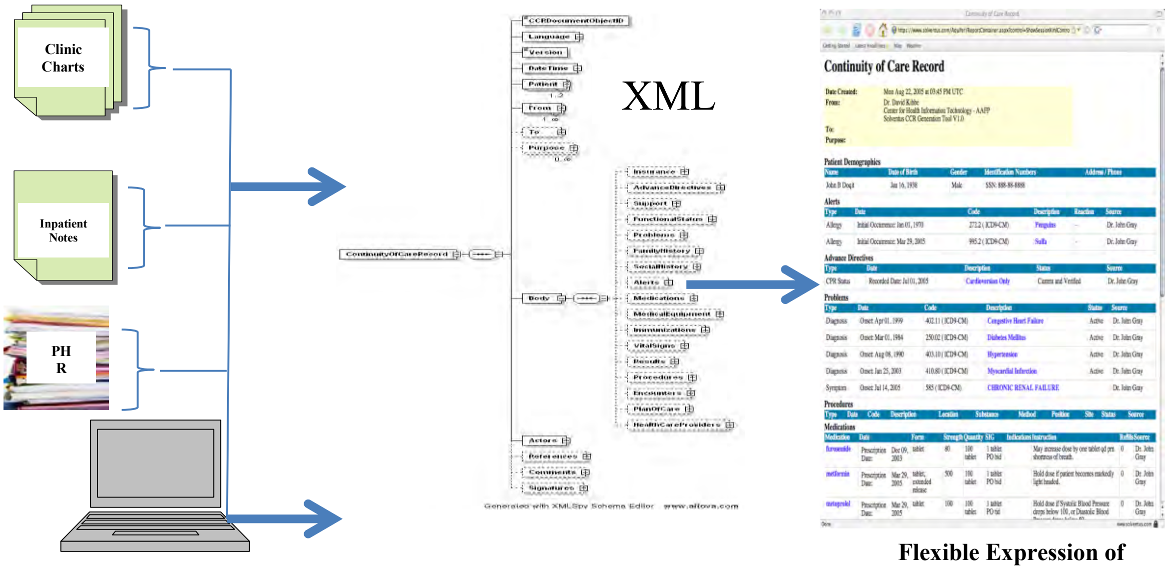


Figure 3.7: CCR/CDA File

Although health system standards emphasize the need for protecting patient's privacy, none of the standards mentioned above provide enough guidance as to how such protection can be achieved. A mechanism for controlled access to Patient's PHRs, which restricts access to only legitimate users, is necessary to ensure patient privacy.

3.12 Privacy and Security of PHR Systems

Although PHR systems may indeed promote communication between patients and their healthcare providers, they also generate new security and privacy issues (Win et al., 2006; Kaelber et al., 2008; Avancha et al., 2012). One of the greatest concerns of the patients in every type of electric healthcare applications including PHRs is the issue of security and privacy of their health records (Win et al., 2006; Kaelber et al., 2008; Zheng, 2011). For example, a working group sponsored by the Markle Foundation conducted a consumer survey of PHR systems, and ninety-one percent of the respondents reported that they are "very concerned" about the privacy and security of their personal health records (Markle Foundation, 2003).

Given that the focus of this section is on privacy and security of PHR systems, it is essential that we clearly define both terms within the context of healthcare. The National Committee for Vital and Health Statistics (NCVHS) described privacy as the user's right to "control the acquisition, uses or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" (Cohn, 2006).

Like any other electronic healthcare application, privacy is one of the greatest concerns of the patients in PHR systems (Win et al., 2006; Avancha et al., 2012). PHR systems support a wide range of health related functions such as: sharing personal health records with the healthcare provider, (to support patient-doctor relationship); empowering patients with chronic conditions see their progress over time; and also encourage good health practices (Kaelber et al., 2008). In such settings, privacy becomes a complex issue. Patients need subtle control over the dissemination and access to their personal health records (Markle Foundation, 2003).

Avancha et al. 2012 identified and described three different types of threats[12] to PHR: (1) Identity threats (misuse of patient identities), (2) Access threats (unauthorized access to PHR) and (3) Disclosure threats (unauthorized disclosure of PHR). When these threats are realised in any PHR system, the consequences may result into exposure of identifiable personal health data, which leads to loss of reputation, harm to health or even death

There are two main concerns related to patient's identity. First, the patient may lose his/her identity credentials, enabling unauthorised users to have access to patient's PHR. This may compromise patients' privacy, since unauthorised users may read, modify or even disclose the patient's health records. Furthermore, insiders may use a patient's identity for medical fraud or malicious damage. In the following section, the researcher review literature related to authentication and cryptographically enforced access control methods, which preserve patient's privacy.

3.12.1 Authentication Method

In healthcare settings, authentication is the process of determining whether: (1) the legitimate patient is being detected; (2) the authorised provider(s) have access to the medical records and (3) the patient's health records are sent to the authentic PHR system (s). Authentication is a foundational technology that impacts patient's privacy. Without authentication, PHR systems cannot provide correct patients' information and controls. Authentication failures expose

[12] Threat to user privacy is the possibility that the user's right to control his\her PHR is weakened or eliminated due to erroneous or malicious actions

health records to disclosure and/or modification. Poor authentication interfaces can also be troublesome, because they encourage unsafe user behaviours such as password sharing (Avancha et al., 2012).

Studies conducted by Citizenship and Immigration Canada (2003), and Furnell and Dowland (2000) found that user IDs and passwords are the most widely used authentication methods, and are often rated highly in terms of user acceptability. The methods don’t require patients to carry any extra hardware device, and they can be changed at the user's choice. Among the PHR systems that deploys user IDs and password methods include Microsoft’s HealthVault and PHRAnywhere. First time users register for the service and the system verifies the user’s entered data against the information provided by the employer. Members are then issued a user ID and password, which they use for subsequent log-ins. In addition, users can also sign in with OpenID accounts in order to offer a second-factor authentication via a physical USB keys. Other companies such as Fujitsu use biometric tool called PalmSecure technology to provide authentication to PHR (Moore, 2009).

3.12.2 Public Key Infrastructure (PKI) for Authentication

Public Key Infrastructure is mainly used with smartcards (Dwivedi et al., 2003; Sax, Kohane, & Mandl, 2005). The smartcards stores encrypted certificates that are issued by the PKI provider along with other relevant information in order to provide robust user authentication (Dwivedi et al., 2003). Smartcards are widely used in healthcare, mostly in Germany, France and Belgium (Cross, 2000; Dwivedi et al., 2003). Healthcare providers use a combination of smartcards and PKI technology to generate patient’s prescriptions electronically (Dwivedi et al., 2003). In addition, through the application of PKI technologies, it is possible to generate unique digital signatures for each healthcare professional and patient’s records (Petrogiannis, 1999).

Although the application of PKI technologies offers robust user authentication and strong digital signature support, there are number of obstacles to consider. First, there is pre-enrolment problem. Users (Sender and recipient) must have a certificate before communication takes place. In an environment where patients don’t have specific healthcare provider(s), this may not be possible. Secondly, the sender must obtain the certificate of the recipient, which is published via a directory. This introduces the problem of trust and information leakage (Housley & Polk, 2001). Finally, while the binding between certificate and identity was true at the time of issuance, there is no guarantee that it remains true after that single point in time.

The sender should confirm first the validity of the recipients' certificate before sending the encrypted data. This is called certificate revocation problem (Voltage security report, 2013).

The problems of certificate revocation have been in existence for many years. Before communication takes place, potential senders should be in position to obtain and ascertain the validity of all the potential recipients. Even if the recipients have certificates, the validity of these certificates must be determined before the data is sent. Approaches for checking the status of the certificate have been to deploy an online certificate status server, which must be accessed by all the senders of the data or publishing certificate revocation lists (CRL's), which must be frequently updated. In both cases, the servers must be online all the time in order to validate the status of the recipients' certificate. All these requirements introduce complexity of the key archive processes.

3.13 Authentication-Based PHR Systems

In addition to user IDs and password methods described above, some PHR systems implement role-based access control (RBAC) scheme to manage user's access rights (Zheng, 2011). The RBAC scheme usually places full trust at the server in order to protect patient's records. The server runs a RBAC program that verifies the request and determines the access rights. A user with appropriate permission(s) is able to access patient's records. Two of the typical examples of authentication-based PHR system include: the Indivo and PCASSO platforms (Adida, Sanyal, Zabak, Kohane, & Mandl, 2010; Mandl, Simons, Crawford, & Abbett, 2007; Mohan et al., 2009).

3.13.1 The Indivo Platform

Indivo is an open-source, and professionally developed personally controlled health record (PCHR) system that enables patients to own and manage their personal health records. It has all the major features that users might hope to see in a PHR system. It provides legitimate users the ability: to add any document patients "feel" may be relevant; support the sharing of patient's records among healthcare providers and patients; and limit patients to edit records that were contributed by the providers. This has given confidence to the healthcare providers that information included in patients' record was not altered by the patients (Mandl et al., 2007).

Indivo is an online system, provides a World Wide Web interface, and built to public and open standard (Mandl et al., 2007). It allows users to create and manage their personal health records, basing on the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Indivo's implementation concept was to provide complete and secure PHRs to patients. Indivo is a three-tier system with data storage tier, a business logic tier, and the user interface. Figure 3.8 below describe the three-tier architecture of the system. The security of patient's health data is enforced at all the three tiers of the system (Mandl et al., 2007). Patient's health data are encrypted and stored at the Indivo backend server. The server is responsible for managing authentication, making health records available to client applications via the Indivo API, and also determines which records are available to which users (Mandl et al., 2007).

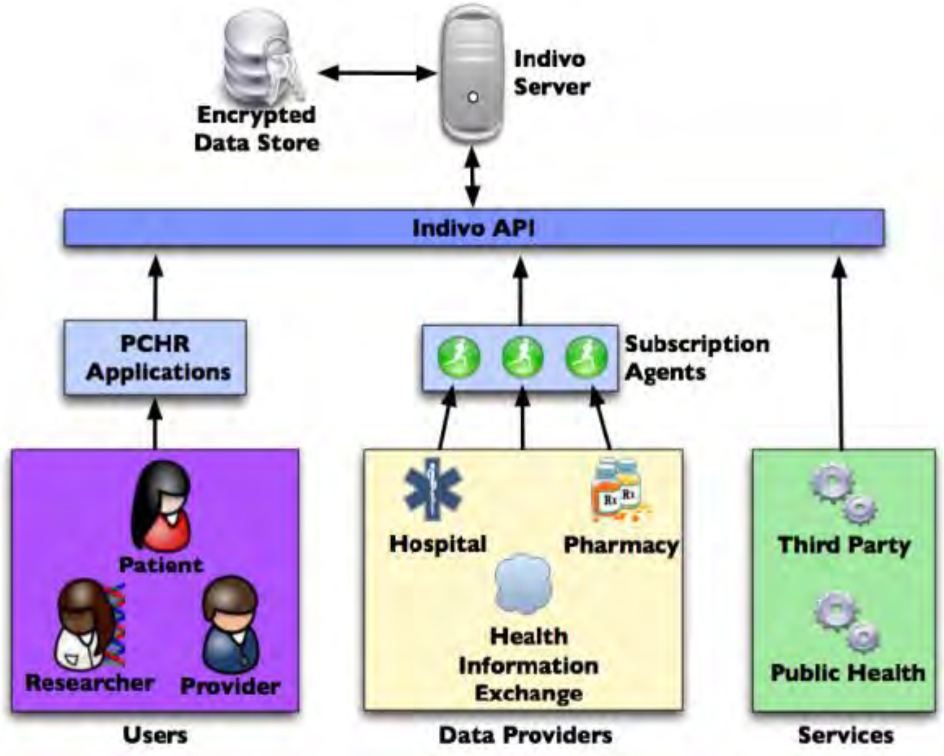


Figure 3.8: Indivo Architecture, demonstrating sources of data; the three tiered architecture and users that access the Indivo server (Mandl et al., 2007)

The Indivo Server provides two classes of security policies: the institutionally-oriented, server-based and user-based security policies. An institutional policy allows users assigned to a particular role to create new accounts. A user-based policy enables a patient to indicate which other users such as providers and researchers have particular privileges on specific portions of their record. These policies are enforced by the Indivo Server along with the institutional policies (Mandl et al., 2007). Unlike Microsoft Health Vault, the Indivo data are stored in XML documents including core Indivo schemas and supported standards.

The Indivo server uses the data storage tier to support the storage of health records. The data storage tier is encrypted to protect the patient's data. Encryption keys are hosted on a separate physical server in order to prevent the decryption of patient's data if the storage device is compromised (Mandl et al., 2007). Although Indivo provides tighter security on patient's records, it does not provide the desired way to enforce patient-centric access control (Zheng, 2011).

3.13.2 The Patient-Centered Access Control Secure System Online (PCASSO) Project

The Patient-Centered Access Control Secure System Online was designed to provide secure access of personal health records over the Internet (Baker & Masys, 1999). The PCASSO architecture secures data from the point of original all the way to the recipient (Baker & Masys, 1999). The PCASSO architecture uses a role-based access control and a user authentication approach to preserve the patients' privacy.

3.13.2.1 Authorisation and Role Based Access Control

The PCASSO architecture allows users to be associated with one or more roles, which defines the level of patients' data other users can see with least privileges and explicit authorisation. A role is typically a job function that gives a user certain privileges with respect to patient's records (Ferraiolo et al., 2001; Kayem, 2008). For example, a user with a doctor's role can only read the data with clearance for doctors. The PCASSO architecture empowers the patient to grant access to only a specific potion of their records. Access is based on user role(s) using labels. Healthcare providers can have full access to patient's data only when they assume the role of emergency (Baker & Masys, 1999).

3.13.2.2 PCASSO Authentication Methods

The PCASSO architecture requires users to have a username/password and public/private keys (details in the next section) in order to respond to a challenge from the PCASSO server (Baker & Masys, 1999). The digital certificate located on a removable medium such as a flash disk is used to encrypt the data, and to authenticate the user to the PCASSO server (Baker & Masys, 1999). After authentication of the user to the PCASSO server, the server and the user exchange a symmetric key, used to encrypt the data flowing between the server and the user. The

PCASSO uses SSLv3, which is widely accepted in healthcare as a strong mechanism for transmitting health data over the Internet (Baker & Masys, 1999).

In a resource constraint setting, some of the reviewed authentication technologies may not be appropriate to preserve patient's privacy. Authentication technologies such as smart cards and physical USB keys are expensive in terms of cost and maintenance (Dagorn, Bernard & Varrette, 2005; Chadwick, 1999). Additionally, smart card technologies don't support mobility (mobility is only possible if the machine that the user accesses has a smart card reader attached, and some machines don't support the same standard of smart card readers). Similarly, physical USB-keys present privacy issues when the USB is stolen (Kao, Luo, Lin, Huang, & Yuan, 2011).

Similarly, all the authentication-based PHR systems described above relies on an online server that maintains an access control authorities. The server only grants access to the user (s) when user's attributes corresponds to the characteristics of the information maintained by the server. The drawback of this approach is that it is designed primarily for online PHR systems only.

3.14 Cryptographically Enforced Access Control

Cryptographic access control is a distributed access control paradigm that is designed for global federation of information systems (Harrington & Jensen, 2003). It defines an implicit access control mechanism, which relies exclusively on cryptography to provide security of data. According to Cohn (2006), security refers to the physical, technological or administrative safeguards used to protect information from unwarranted access or disclosure. There are three basic elements of data security: confidentiality, integrity and availability. To establish the level of confidence in the information, providers must securely process confidential information in a way that cannot be disclosed to unauthorised users (Adesina et al., 2011). Therefore, it is the obligation of those who receive end-user information to respect the security interests of the users.

Protecting the integrity of information means maintaining and assuring the accuracy and consistency of the information over the entire life cycle (Boritz, 2005; Adesina et al., 2011). Inaccurate information can be a serious problem and can lead to disastrous situation. Availability is an integral component of data security, which determines whether the information is available for use by its intended users (Tanenbaum & Van Steen, 2002). All means such as computing devices for accessing the information should be available to end-users whenever the need arises (Adesina et al., 2011).

3.14.1 Public Key Cryptography

According to Akdeniz (1996), cryptography is the science and study of secret writing. It concerns the ways in which data can be encoded to prevent disclosure of their contents through eavesdropping or message interception (Diffie & Hellman, 1976). Cryptography provides technologies that store sensitive information, and transmit it across insecure Internet such that no one can read, write or modify the information except the intended recipient (Diffie & Hellman, 1976; Akdeniz, 1996). Previous studies by Narayan et al. (2010) and, Sun, Zhu, Zhang and Fang (2011) demonstrate that the most security protocols for electronic health records are based on public key cryptography.

3.14.2 Overview of Public Key Cryptography

The concept of Public Key Cryptography was introduced by Diffie and Hellman in 1975 to solve the problem of key distribution (Diffie & Hellman, 1976). The aim was to make key distribution easier in a multi-user communication network. Public key cryptography is an asymmetric scheme that uses a pair of keys: a public key, which encrypts data, and a private key or secret key for decryption. Users obtain both keys, with the private key kept secret (to provide privacy) and public key publically known. Figure 3.9 illustrates the process of public key cryptography. A user publishes his public key while keeping the private key secret. Any person with a copy of the user's public key can encrypt the information. The primary benefit of public key cryptography is that it allows users without pre-existing security arrangement to exchange records securely. This means that the sender and receiver share the secret keys with no secure channel dependency. Communication involves only the public key and no private key is ever transmitted (Diffie & Hellman, 1976; Goldreich, 2004).

Similarly, Public Key Cryptography provides technologies\methods that support digital signature and digital certificate (ElGamal, 1985). Digital signatures allow the recipient to verify the authenticity of the information's origin and ensure that the information is intact (ElGamal, 1985; Goldreich, 2004). This therefore means that public key digital signatures provide authentication, data integrity and non-repudiation.

The drawback of the earlier technologies of digital signature is that it is slow, and produces enormous volume of data (Ferguson & Schneier, 2003). It is therefore because of this reason that Diffie and Hellman (1976) introduced the concept of one-way hash function. A one-way hash function takes the variable length as an input. The message of any length produces a fixed-length output (n-bits). The goal is to ensure that, if the message is changed in any way, an entirely different output value will be produced and thus causing digital signature verification process to fail.

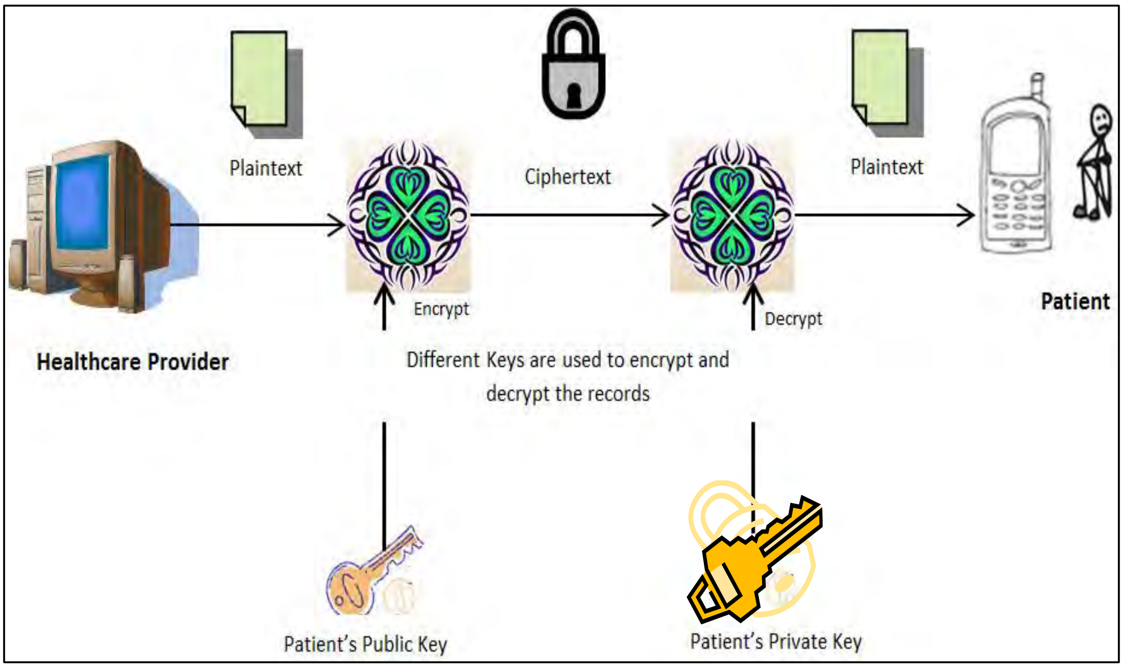


Figure 3.9: The process of Public Key Encryption

3.14.3 Digital Certificates

The greatest challenge with public key cryptosystems is to ensure that the public key to which the sender is encrypting the data is in fact the public key of the intended recipient (ElGamal, 1985; Naor & Yung, 1990). Similarly, if the sender of the information wishes to exchange the information with the people he has never met; it becomes impossible to assume that the sender has the correct key. Digital certificates were introduced to simplify these tasks by establishing whether a public key truly belongs to the purported owner. A digital certificate is a signed assertion about a public key. More specifically, a digital certificate is information embedded with a user's public key to help other beneficiaries verify that a key is genuine or valid. They function much like a physical certificate such as the user's driving permit, social security card or birth certificate. Each of these certificates has some information that identifies the owner, and authorisation showing that someone else has confirmed the owner's identity.

Digital certificates consist of three major components;

1. A public Key
2. Certificate information that identifies the owner such as ID, or name of the owner
3. One or more digital signatures

Thus, a digital certificate basically is a collection of identifiable information bound together with a public key, and signed by a trusted third party to prove the authenticity of the owner. This means that for a group of people wishing to communicate securely, it is necessary to put more structured systems in place to provide additional key management features. These systems called Public Key Infrastructure contain the certificate storage facilities and provide certificate management facilities (such as issuing, revoking, storage and retrieval). The main feature of the Public Key Infrastructure (PKI) is the introduction of the Certification Authority (CA). A Certificate Authority is responsible for creating certificates and digitally signs them using the CA's private key (Sax et al., 2005; Lysyanskaya, Rivest, Sahai, & Wolf, 2000).

3.14.4 PKI for Encryption

Certificates in Public Key Infrastructure systems are used to bind encryption keys to user identities via the registration process. The process is combined with digital signing technologies in order to produce a digital certificate. When this process is tightly controlled, a digital certificate can provide an assurance that intended users can access the encrypted data with the key contained in the certificate. The potential sender of the encrypted data must obtain the certificate of the recipient in order to communicate securely with the certificate holder (Szolovits & Kohane, 1994; Sax et al., 2005). Figure 3.10 describes the process of certificate-based encryption scheme.

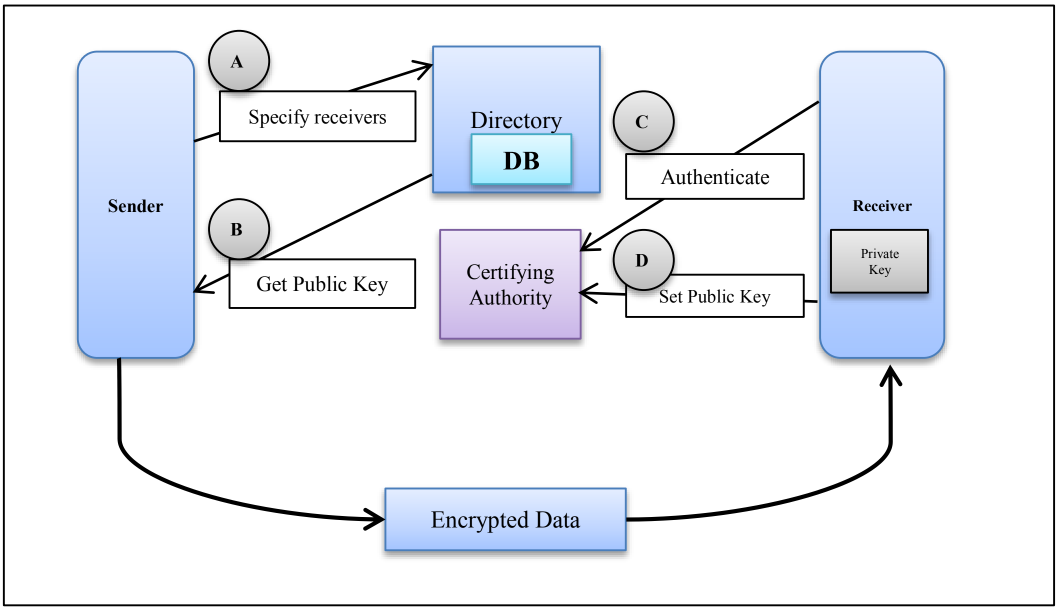


Figure 3.10: The process of Certificate-Based Encryption

From Figure 3.10, certificates are authenticated data structures that tie a receiver's identity to a public key. Because they are authenticated, certificates are stored on distributed untrusted directory. This splits the key management server into a public facing directory and a Certifying Authority. The Certifying Authority is the only trusted component responsible for creating certificates.

While PKI is well suited to underpin strong authentication and encryption mechanism, it is not an ideal infrastructure for healthcare service particularly in developing countries. The hurdles are over overwhelming, and are all linked to the complexity of managing user certificates and key management. The issuance, verification and revocation of digital certificates are critical tasks and can introduce management burdens, especially for hospital administrators and end-users including the patients. This was well recognised by Shamir far back in 1984, and the concept of Identify-Based Encryption (IBE) was introduced (Shamir, 1984). With Identify-Based Encryption, user identities such as email address, phone number and date of birth are used as encryption keys (Shamir, 1984). This completely obviates the need for key management and digital certificates (Shamir, 1984; Garson & Adams, 2008).

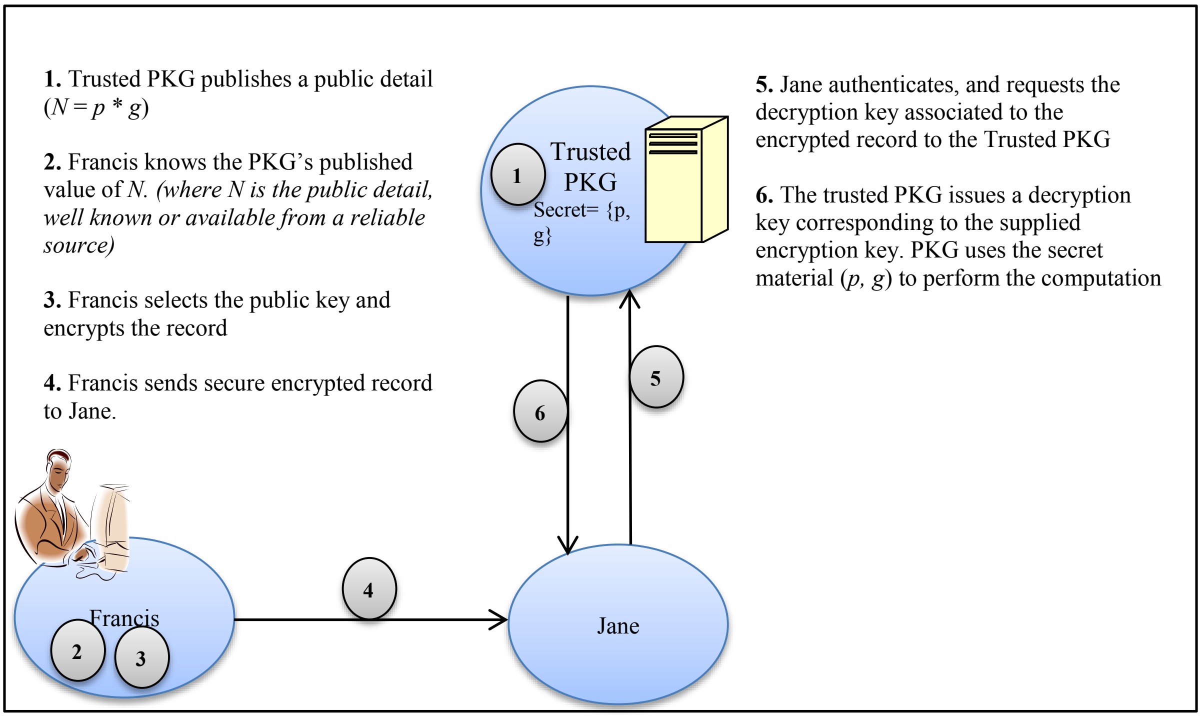
3.15 Identify-Based Encryption

Identity-Based Encryption (IBE) is a paradigm introduced by Shamir in 1984 (Shamir, 1984). His goal was to simplify key management processes and remove the need for public key certificates. With IBE, the public key is set to any string interpreted as one's identity (email address, telephone number, date of birth combined with a user name etc.). The private keys are generated by the trusted authorities called Private Key Generators (PKGs), which delivers the keys to users after deriving them from user identities. End users do not need to enquire for the certificate of their public key. The removal of certificates enables end-users to avoid the trust and certificate management problems encountered in Public Key Infrastructure: binding public keys to its owners are no longer necessary, and simplicity with key management since public keys are human-memorised (Boneh & Franklin, 2001).

There are number of solutions for Identity-Based encryption that have been devised ever since 1984 (Fiat & Shamir, 1986; Guillou & Quisquater, 1990). However, finding a practical IBE solution remained an open research problem until 2001 when elegant solution was provided by Boneh and Franklin, and Cocks (Boneh & Franklin, 2001; Cocks, 2001).

Basically, an identity-based cryptosystem consist of two core properties;

First property: Any string can be used as an Identity-Based Encryption/ public key. The string should consist of any sequence of characters such as a name combined with the data of birth, a text, an email address or a list of terms and conditions. The data/records are encrypted by using this string along with the "public detail", which is associated with a trusted key server called the Private Key Generator (PKG). The PKG is the only entity that generates the corresponding private key.



1. Trusted PKG publishes a public detail ($N = p * g$)

2. Francis knows the PKG's published value of *N. (where N is the public detail, well known or available from a reliable source)*

3. Francis selects the public key and encrypts the record

4. Francis sends secure encrypted record to Jane.

5. Jane authenticates, and requests the decryption key associated to the encrypted record to the Trusted PKG

6. The trusted PKG issues a decryption key corresponding to the supplied encryption key. PKG uses the secret material (*p, g*) to perform the computation

Figure 3.11: The IBE interaction model

Second property: The generation of the private key (associated with a string) can be postponed in time. This means that, a private key can be generated at a later date/time after the creation of the corresponding IBE encryption key.

Figure 3.11 shows the IBE interaction model. The model involves three players: a sender of an encrypted record (Francis), the receiver of the encrypted record (Jane) and a trusted Private Key Generator responsible for issuing private keys. Both Francis and Jane must trust the Private Key Generator (PKG) in order to start communication. Below are the steps Francis and Jane take to complete the secure sharing of the encrypted record;

1. The PKG performs the initialisation phase, generates a secret key (protected and stored at the e.g. hospital server or PKG site) and a corresponding "public detail" that is publicly available.
2. Francis trusts the PKG or the hospital server and retrieves the public detail.
3. Francis defines the public key and encrypts the record. The IBE encryption key is any type of string such as Jane's email address. The record is encrypted using the IBE encryption key and the PKG's public detail.
4. Francis sends the encrypted record to Jane.
5. Jane authenticates to the Private Key Generator and requests the decryption key associated to the encrypted record. Jane must provide her credentials in order to prove to the PKG that she is the legitimate receiver of the record.
6. The PKG generates and issues the private key to Jane, if it was satisfied with Jane's credentials. The PKG can also generate private keys depending on the conditions specified by for example the hospital administrator.

Thus, the IBE model can fit well in securing personal health records. First, it is possible to use end-user's credentials such as phone number, name, combined with date of birth as an IBE encryption key, and directly encrypts patient's records. Secondly, the PKG can generate the corresponding private key if the patient's credentials are satisfied by the PKG. Besides, there is no need to share or store any secret between the patient and healthcare provider. Similarly, if the physician or clinical officer is revoked or leaves the hospital, the PKG will automatically stop issuing new private keys. The fired physician or clinical officer will not be able to re-authenticate to the PKG since his/her account will be disabled. Thus, the hospital administrator needs to do nothing special, unlike in PKI systems.

3.16 Cryptography-Based PHR System

The majority of PHR systems are based on public key cryptography (Zheng, 2011; Li, Yu, Zheng, Ren, & Lou, 2013; Wang, Liu & Li, 2012; Hsieh & Chen, 2012; Parameswaran, Vanitha, & Arvind, 2013). These systems allow patients to encrypt their personal health records and distribute the corresponding decryption keys to the authorised end-user. Typical examples of cryptography-based PHR systems include MedVault platform and iHealthEMR system.

3.16.1 The MedVault Platform

The MedVault system is an online system that implements a patient-centric sharing framework for PHRs. It provides an online attribute-based authentication system, which requestors of the patient's record must possess. Attribute providers (APs) are entities that verify users' attributes and certify them. The APs create digitally signed credentials and provide them to the users (Mohan et al., 2009). Figure 3.12 below describes the system architecture of the MedVault sharing framework.

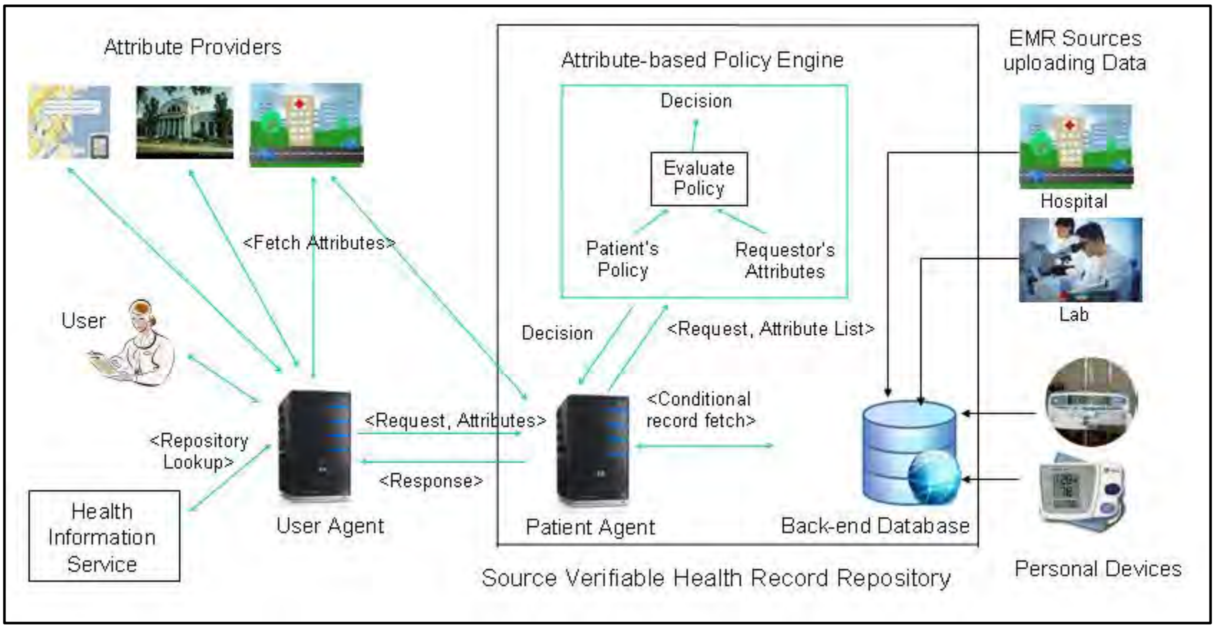


Figure 3.12: Architecture of MedVault sharing framework (Mohan et al., 2009)

The health records reside in a secure provable repository. If a user wishes to access the records of a particular patient, the requesting user connects to his agent using the web browser. The user agent makes access requests to the patient agent on the user's behalf. The Health Information Service (HIS) allows the querier to locate the available repositories and the types of records available for the patient in question. Upon receiving a request from a user agent, the patients' agent notifies the user agent of the attributes required to complete the access. Both the patient agent and authorisation module are co-located with the repository. The patient agent sends the health record information to the user agent, which normally relays it back to the user's device.

The MedVault sharing framework was designed with a large and high-level infrastructure in mind (Mohan et al., 2009). It assumes that all cryptography used is secure and that, there exist a trusted PKI infrastructure for healthcare professional, patients and other licensed entities (i.e. insurance companies).

3.16.2 The iHealthEMR System

The iHealthEMR system was designed by Akinyele et al. 2011 to provide self-protecting electronic health records using Attribute-Based Encryption (Akinyele et al., 2011). The system allows patients to encrypt each node in the XML-based EHR access policy before exporting it to cloud system. End-user's access rights are defined by the attributes within their private key. However, the architecture does not solve the practical problems of key revocation and key delegation. Additionally, the evaluation of iHealthEMR system was limited to short-term laboratory studies using laboratory experiments. Previous studies have shown that the results from laboratory studies may not necessarily apply in the real-world contexts in which the tools are to be used (Mugwanya, 2013). Therefore, it is not clear whether iHealthEMR can be used by patient-users in real world context.

Furthermore, despite recommendations that patients be involved in the design and testing of healthcare technologies (Hurtado, Swift, & Corrigan, 2001), and that a full description of how healthcare technologies for patients were designed and tested be included in the report (Gustafson, Robinson, Ansley, Adler, & Flatley-Brennan, 1999), none of the studies described above provide a complete description of how patients were involved throughout the development process. Therefore, this study describes how patients are involved in the design and testing of an interactive PHR system, right from the requirement analysis stage to the final evaluation.

3.17 Beyond Cryptography and Authentication Approaches

Beyond cryptography and traditional authentication approaches, Daglish and Archer (2009) described two approaches that can be used to secure electronic health records over the Internet:

Network encryption and Secure Socket Layer (SSL). In the next section, we discuss these approaches and choose the best option for PHR security.

3.17.1 Network Encryption

Network encryption is a network security process that applies crypto services at the network transfer layer (Ding, Pang, Fang, & Peng, 2007). The importance of network encryption was noticeably increased due to the constant increase in the number of clients that depend on the benefits provided by the wireless networks (Barka et al., 2006). The fact that wireless communication is based on broadcast radio frequency (RF), critical questions related to the security of communication on wireless networks appears.

The introduction of Wired Equivalent Privacy (WEP) protocol specifically implemented for wireless networks provided an enhancement to the confidentiality and integrity between different parties (Barka et al., 2006). WEP is an optional IEEE 802.11 feature that prevents disclosure and modification of data while in transit. It provides a mechanism where a person sets up a 128-bit security key that is shared between the mobile device and an access point. WEP uses the RC4 as its underplaying algorithm. When it is enabled, each “station” is given a key. The key is used to scramble the data before transmission. Once the station receives the data that is not scrambled with the appropriate key, it discards the data and rejects the request. Figures 3.13 (a) and 3.13 (b) describes the encryption and decryption processes of WEP. To protect against unauthorised data modification, an integrity algorithm (CRC-32) operates on the plaintext to produce the integrity check value (ICV) (Saleh & Al Khatib, 2005).

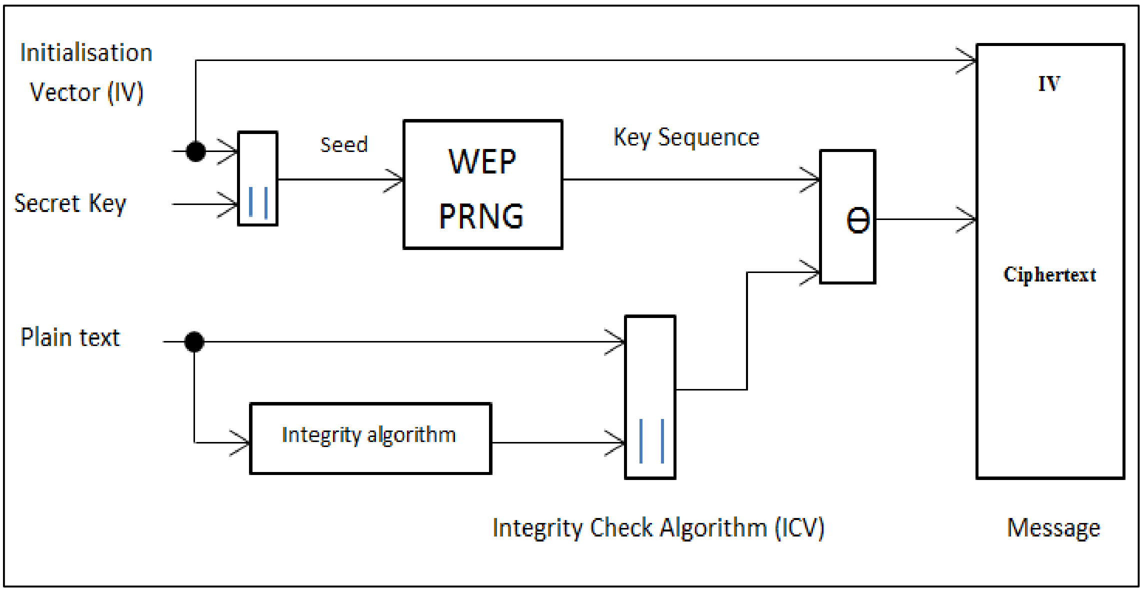


Figure 3.13 (a): WEP Encryption Algorithm

There are two processes that apply to plaintext data during WEP encryption. The first process involves plaintext encryption and the second process includes protecting the data against unauthorised data modification. Typically, the encryption process begins with a plaintext message that needs to be protected (Vines, 2002; Boulmalf, Barka, & Lakas, 2007). Decryption in WEP follows the same process as that in the encryption, but in a reverse order.

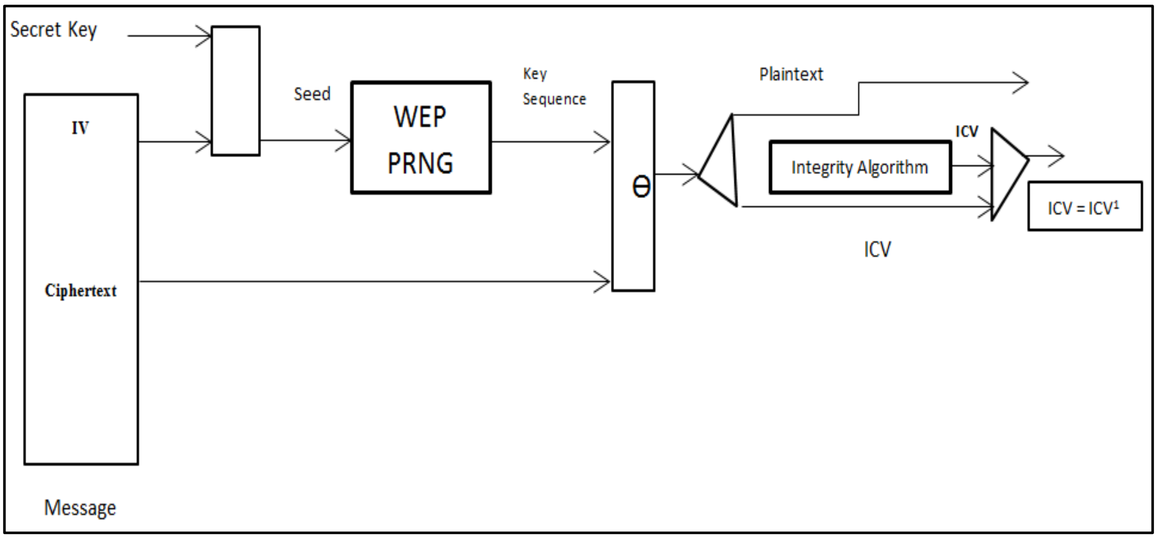


Figure 3.13 (b): WEP Decryption Algorithm

Although WEP provide users with some degree of protection, it is not considered to be secure against a casual eavesdropper attack (Bittau, Handley, & Lackey, 2006; Barka et al., 2006). Therefore, a more secure protocol is needed to protect patient's health records.

A study conducted by Garson and Adams (2008) emphasized that, IPsec and Secure Socket Layer (SSL) can be used to implement a secure EHR system. However, Array Networks, (2003) noted earlier that, IPsec is a notoriously complex protocol to configure and manage. In the meantime, SSL is a much easier alternative to IPsec. Its implementation has proved to be more secure not only in healthcare IT systems, but also in other systems (Hiltgen, Kramp, & Weigold, 2006; Oppliger, Hauser, & Basin, 2008; Garson & Adams, 2008; Dmitrienko et al., 2011; Takemura et al., 2012; Bahga & Madisetti, 2013).

3.17.2 Secure Socket Later (SSL)

The Secure Sockets Layer is a commonly used protocol for managing the security of data over the Internet (Win et al., 2006; Mandl et al., 2007; Zhang & Liu, 2010). SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. It uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

The Secure Sockets Layer uses a handshake protocol to establish a shared key between the patient's device such as mobile phone and the server (Garson & Adams, 2008). The shared key is used to encrypt the data before communication takes place. This creates an "encrypted channel" between the user-device and the server. SSL can be used to provide secure communication and authentication (Zhang & Liu, 2010; Oppliger et al., 2008). In the first case, no certification authority is required. The server only transmits its self-signed certificate to the user's application in order to encrypt the data (Zhang & Liu, 2010). In the latter case, the Certificate Authority (CA) is needed in order to authenticate the server and the end-user application (Oppliger et al., 2008). This adds unnecessary cost such as the certifying authority's subscription fee for issuing the digital certificate in order to provide secure access of information.

3.18 Security and Usability

There is an old joke that was highlighted by Karat, Brodie and Karat (2005) that "computers are actually easy machines to secure: just turn them off, lock them in a metal-lined room, and throw away the key. What you end up with is a machine that is very secure…" Of course they may be secure, but not usable. In addition, while they may be secure, users who need to use them may prefer to use other devices with significantly weaker security model. Similarly, Karat et al. (2005) explain that if people are unable to use secure computers, they will use computers that are not secure but usable. This means that computing devices that are theoretically secure, but not usable, will do little to protect end-user's personal information.

3.19 Usability in the Privacy and Security Domain

The most used definition of usability was given by Nielsen in 1993. According to Nielsen (1993), "usability is about learnability, efficiency, memorability, errors, and satisfaction". Other standard definitions of usability after 1993 describe usability as the measure of the ease with which a system can be learned and used, including its effectiveness, safety and efficiency (Preece, Rogers, Sharp, Benyon, & Holland, 1994; ISO 9241-11, 1998).

Typically, usability is measured by test users (selected to be as representative as possible of the intended users) to discover errors and areas of improvement in the pre-specified set of tasks, or measure by having real users in the field perform their day-to-day tasks (Nielsen 1993; Jones & Marsden, 2006). In either case, the key point is that usability is measured relatively to certain tasks and certain users.

3.20 Design for Usability and Security

According to Roger (2004), there are a variety of research designs and methodologies that are proposed by Human-Computer Interaction (HCI) experts. However, bridges.org advocates for user-centric approaches to create appropriate technologies for end-users specifically in the developing world (Peters, 2001). In the next section, we describe some of the user-centric approaches in ICT4D design initiative.

3.20.1 Human-Computer Interaction

Back in 1960s, computer vendors viewed end-users as no more than an inconvenience, and most of the work was concentrated on "user friendly" system (Nielsen, 1993). However, in the early 1980s, researcher noted that users don't need machines to be friendly to them. Instead, they need machines that will help get their work done (Card, Moran, & Newell, 1980). Because of this, user interface professionals have tended to use other terms such as Human Computer Interaction (HCI). Human computer interaction professionals study humans and computers concurrently. It involves activities such as planning, studying and design of the interaction between end-users and computers (Helander, Landauer, & Prabhu, 1997; Preece et al., 1994; Jacko & Sears, 2003).

Field studies and requirement analysis are valued practices in the HCI communities (Kujala, Kauppinen, Nakari, & Rekola, 2003). Field studies are characterised by taking place in the "real world" as opposed to in a laboratory setting. This means that design and experimentation are carried out as users go on with their normal duties. This provides data about what people really do and how a new system and its interfaces should be designed. Kujala et al. (2003) described that combining HCI and field studies (including contextual inquiry) provide a real opportunity to improve usability and system quality.

3.20.2 User-Centered Design

User-Centered Design (UCD) also known as Human-Centered Design (HCD) is a design process in which the user is at the centre of the design process. UCD aims at obtaining a high quality system that satisfies the end-users. UCD is a multi-disciplinary approach to interactive system that focuses specifically on making systems usable based on user requirements and their tasks at hand (Abras, Maloney-Krichmar, and Preece, 2004; Jones & Marsden, 2006). While HCI looks broadly at the design of the product, UCD focuses on the user as a co-designer.

Gould and Lewis (1985) described three guiding principles of UCD:

1. **Focus on users and tasks early and throughout the design process:** This is the first principle that requires direct contact with users' right from the information gathering stage so as to understand the cognitive and physical characteristics of the users in their environment.
2. **Measure usability empirically:** Measuring usability empirically is the second principle that calls potential users to get involved in the simulating activities and processes that are to be performed by the system. This principle involves system testing to ensure that users' cognitive characteristics are matched with the system.
3. **Design and test usability with users in an iterative manner:** This is the last principle that requires that there must be a cycle of assessing-designing-testing-analyzing-refining-testing-analyzing-refining-testing until users are satisfied with the system. Thus, the system functions are changed continuously depending on the results of the last testing.

Additionally, the international standard ISO 13407: Human Centred Design Process for Interactive Systems describes four activities of Human-Centred Design, illustrated in Figure 3.14;

1. Understand and specify the context of use
2. Specify user and organisational requirements
3. Produce more than one candidate design solution
4. Evaluate designs against requirements

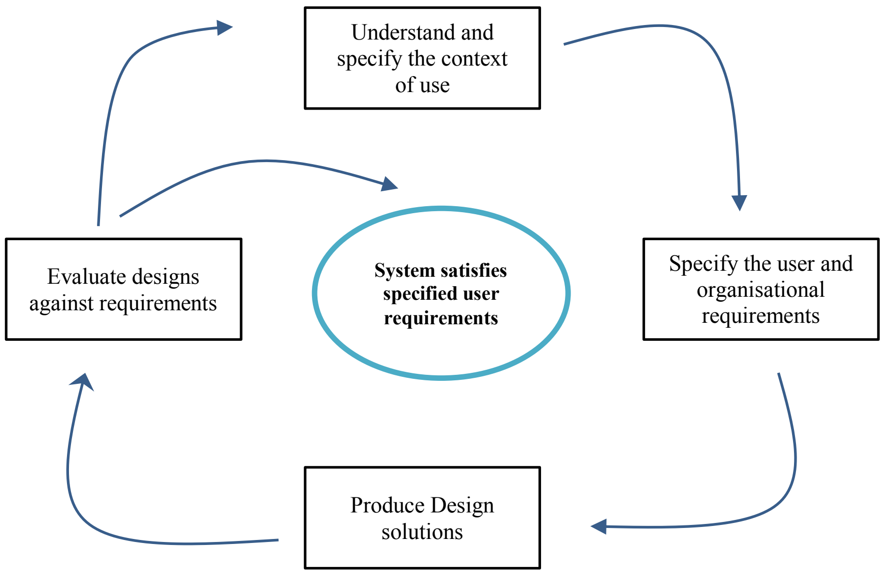

Understand and specify the context of use
Specify the user and organisational requirements
Produce Design solutions
Evaluate designs against requirements
System satisfies specified user requirements

Figure 3.14: Activities of Use-Centred Design

The first activity involves knowing the user, the environment of use, and the tasks that the beneficiaries use the product for. This is called contextual analysis (Holtzblatt, Wendell, & Wood, 2005). The second activity involves transforming the contextual data into a detailed requirements specification. The activity also determines the success criteria of usability for the product in terms of user tasks, e.g. how quickly a typical user should be able to complete a task with the system. The third activity involves incorporating HCI knowledge of interaction design and usability into a prototype design, followed by an evaluative phase where the user experiences the prototype. These activities require looping back to earlier stages so that development occurs in iterative cycle (Gould & Lewis, 1985).

Preece et al. (2002) highlighted various techniques describing how to involve users in the design and development of the product or artefact: interviews and questionnaire, focus group, on-site observation, walkthroughs and simulations. Table 3.2 describes the purpose of each method (s) and the stage of the design cycle to which the methods can be applied.

Table 3-2: Involving users in the design process (adapted from Preece et al. 2002)

Technique	**Purpose**	**Stage of the design cycle**
Background interviews and questionnaires	Collecting data related to the expectation and needs of users, evaluation of the design alternatives,	This is done at the beginning of the design project

	prototypes and the final product	
Sequence of work interviews and questionnaires	Collecting data related to the sequence of work to be performed with the system	This is done early in the design cycle
Focus group	Comprises stakeholders to discuss issues, needs and requirements	This is done early in the design cycle
On-site observation	Understanding the environment in which the system will be used	This is done early in the design cycle
Walkthroughs and simulations	Evaluation of design (prototype) alternatives to gain additional information about user needs and expectations	This is done early and mid-point in the design cycle
Usability testing	Collecting measureable data related to usability criteria	This is done at the final stage of the design cycle
Interviews and questionnaires	Collecting qualitative data related to user satisfaction with the system	This is done at the final stage of the design cycle

3.20.3 Participatory Design

Participatory design (PD) is part of the first activity in the ISO 13407: Human Centred Design activities. It is an approach to design that actively involves all stakeholders in the design process in order to ensure that the designed system is usable and meets the needs of the stakeholders (Kensing & Blomberg, 1998; Schuler & Namioka, 1993; Muller & Kuhn, 1993). Participatory design was first adopted in Scandinavia as an approach of workplace democracy in decision-making. It is an approach that captures not only the user's information flow but also regarded as a dimension for user empowerment and democratisation (Schuler & Namioka, 1993).

Participatory design is broken down into three stages: Initial exploration, discovery process and prototyping (Spinuzzi, 2005). Figure 3.14 describes the interaction of the three phases. During the initial exploration, participants\end-users of the product cooperate with the product designers to help define the problem and focus ideas for solution. Problem identification and specification of ideas are obtained through ethnographic research approaches such as observation and interviews. The discovery process involves understanding user needs and envisioning of the design (Spinuzzi, 2005). Preece et al. (2002) described that using real scenarios at this stage enable users to explore and discuss context, needs and requirements in a representative manner.

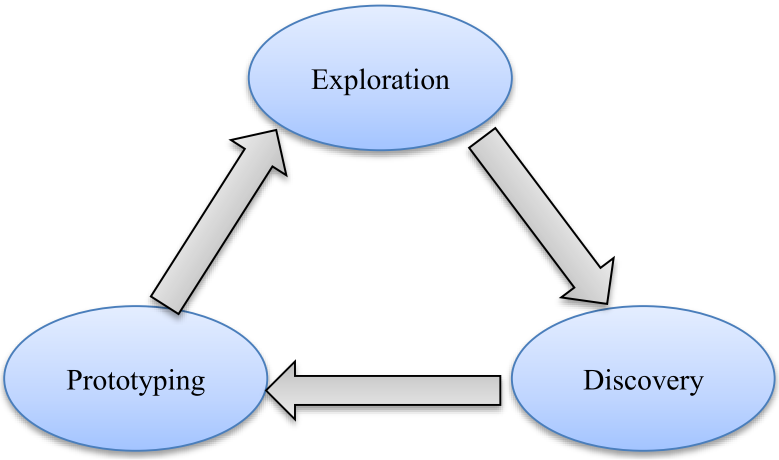


Figure 3.15: Phases of Participatory design

A sketched-out scenario also referred to as a storyboard enables participants to articulate the way the system should work and visualise the use of an interface. The sketches refine and prioritise tasks and actions. Participants can have several iterations of the conceptual model (a representation of storyboards and scenarios) in order to get a stable pattern and recognisable flow. The scenarios on the storyboards form low-fidelity prototypes (Nielsen, 1990).

Prototyping enables developers to cut down on the complexity of the system implementation (Nielsen, 1994d). Users can easily articulate how the system should work through sketches and task flow. Sketching scenarios on paper (paper prototyping) has taken prototyping to the extreme since it reduces the level of functionality and the number of features, which makes it very cheap to design and implement (Nielsen, 1990, 1994d). Additionally, paper prototypes are cheap and user friendly, since they don’t need specialised skill to operate. They support general participation and provide quick and frequent feedback. Paper prototypes can be used to capture system features such as textboxes and radio buttons among others.

3.20.4 Evaluating the Design Solutions

Evaluation is a form of interpretation, which can itself be single or multiple. It is an iterative process that tests the outcome of the design process until a final product is realised. Traditionally, evaluation was limited to testing the final product. However, due to the systems failures that is normally caused by requirements mismatch, ICT4D scholars advocates for evaluation that are made up of iterative reflection of the design processes and their outcomes. Therefore, evaluation is considered not a summative process, but rather a formative process. In the next section, we break down evaluation into requirement analysis and evaluation; iterative conceptual model evaluation; and usability evaluation (Abras et al., 2004).

3.20.4.1 Requirement Analysis and Evaluation

In software engineering life cycle, evaluation is carried out in terms of the requirements elaborated in the first phase of the software development process: requirements analysis. Requirements are taken to be equivalent to `stated needs', consist of expression, discussion and commitment (Mayhew, 1999). Requirement analysis and evaluation ensures that all user needs are captured and nothing is left out.

3.20.4.2 Iterative Conceptual Model Evaluation

Conceptual modelling is a collaborative and democratic process carried out by the users and the designer together, and involves negotiations and presentations of end-user requirements and needs. According to Siau and Tan, (2005), conceptual modelling is aimed at requirements representation and requirements validation. In requirements representation, conceptual models are created to map real-world needs, while requirements validation verifies that end-user needs have been correctly specified, by looking at the generated conceptual models. Hence, the quality of the conceptual model may greatly affect the efficiency, effectiveness, and usefulness of the system. Conceptual model evaluation is designed to get feedback before any code has been developed. This ensures that the transformation from cognitive processes (processes that involve activities such as thinking, remembering and/or reasoning) to physical artefact has captured the totality of internal activities and external interactions (Gitau, 2012).

3.20.4.3 Usability Evaluation

Usability evaluation looks at the final design artefact; the interactions and the user’s experience of using the artefact. The same evaluation principles used in the second level of evaluations

(Conceptual model evaluation) are employed here, except, that at this second level the artefact is complete, while in the second level a paper mock-up was used. The purpose of this evaluation is to assess the final artifact against the usability goals set at the beginning of development (Abras et al., 2004). Therefore, usability evaluation relies greatly on how well the first and second levels of evaluation processes were done.

In conclusion, the design and development of an interactive healthcare technology for patients should be collaborative and support a democratic process between the patients, healthcare givers and the designers. It should involve negotiations of various needs and requirements among different stakeholders. As noted early, continuous evaluation of the product by the end-user at every stage of the technology development should ensure that users are satisfied before proceeding to the next stage.

Similarly, studies have shown that keeping the focus on end-user tasks and requirements throughout the development process helps to reduce the risk of designing an interactive health application that will be considered useless to the users. User-Centred Design (UCD) approach is one of the design methodologies that put great emphasis on understanding user requirements and their environment.

3.21 Summary

Although many interesting findings have been presented in this chapter, the researcher agrees with the view of Kantanka that there is still lack of knowledge in determining the usefulness of PHR system to users in developing countries. Previous research on PHRs has been conducted for developed world, typically focusing on the definition, features and benefits of using such systems. Other studies have proactively focused on the potential challenges and appropriate models for PHR (provider-based PHR, health plan, vendor-supplied and patient-centric model). Similarly, studies conducted by Win et al. (2006), Kaelber et al. (2008), and Avancha et al. (2012) suggest that PHR developers need to more deeply consider potential problems such as designing for security, confidentiality and availability.

In order to design a PHR system that offers high interoperability and security of data, a number of standards and laws have been developed. Among the standards include: Health Language Seven (HL7), Health Insurance Portability and Accountability (HIPAA), Continuity of Care Record (CCR) and Continuity of Care Document (CCD). Current PHR systems support multiple standards and laws, which makes it possible to interoperate with other systems.

Additionally, a study conducted by Avancha et al. (2012) suggests that securing PHRs requires a combination of authentication (to ensure server and patient identities), encryption (to prevent against eavesdropping) and signing (to prevent tampering with PHR contents). Although the SSL protocol to some extent provides authentication and encryption between the patient and the server, it lacks capabilities to protect patient's health records beyond transmission (Win et al., 2006). Similarly, Seltzer (2010) highlighted that authentication through conventional SSL can be weak and subject to man-in-the-middle attacks. Therefore, it is necessary to implement an access control system that manages permissions and access to patient's PHRs. Studies by Mandl et al. (2007); Garson and Adams (2008) and Antón-Rodríguez et al. (2011) acknowledged that cryptographic and data encryption techniques, coupled with SSL, provide secure access of patient's health records. Cryptographic techniques provide confidentiality, integrity and authenticity of the information transferred between different stakeholders, and protects personal health records on the PHR device (Akinyele et al., 2011).

Despite recommendations that patients be involved in the design and testing of healthcare technologies (Hurtado, Swift, & Corrigan, 2001), and that a full description of how healthcare technologies for patients were designed and tested be included in the report (Gustafson, Robinson, Ansley, Adler, & Flatley-Brennan, 1999), none of the previous studies conducted in Uganda provide a complete description of how patients were involved throughout the development process. Therefore, this study describes how patients are involved in the design and testing of an interactive PHR system, right from the requirement analysis stage to the final evaluation.

Applying HCI principles to the design of PHR system is of particular importance, since most patients have not managed their health information electronically before and little is known about the characteristics of the users, which functions they would use the most, and what changes in health-related behaviours will rise from adoption of the technology. Similarly, unlike other healthcare technologies, health and technology literacy are central considerations in the design of the PHR systems particularly in Uganda. Health illiteracy can present users with difficulty in comprehending and managing their health information stored in a PHR (Lober et al., 2006; Kupchunas, 2007). Technology illiteracy can also be a limiting factor in the adoption of electronic PHRs (Lober et al., 2006). Therefore, applying HCI principles to the design and evaluation of the PHR system with special attention to these considerations will enhance functionality and usability, thereby increasing end-user satisfaction and acceptability of the system among the patients.

In our study, we adopt the recommendation of Garson and Adams (2008) and propose an access control framework that protects personal health records on a mobile phone. The framework is designed to augment an authentication-based system, providing PHR protection and access control without the requirement of a centralised server. For cryptographic operations, we demonstrate that Identity-Based Encryption (IBE) is more suitable to achieve patient-centric access control. We also extend other people's work and implement a prototype PHR system based on the IBE scheme.

Moreover, the separation of authentication from cryptographic operations is demonstrated to enable our PHR system utilise existing authentication methods such as PIN to authenticate patients. Consequently, it is possible to dynamically adjust the authentication method as the need arises (Voltage security report, 2013).

In the next chapter, we report patient-user requirements and needs, which were used in the later chapter to design an access control framework that protects personal health information on the mobile phone.

“A dream without a plan is only a daydream”

- *John Maxwell*

CHAPTER FOUR: CONTEXTUAL INQUIRY WITH PATIENTS AND HEALTHCARE PRACTITIONERS

4. Introduction

In this chapter, we present a contextual inquiry study conducted with patients and the clinical officer at Allan Galpin Health Centre (AGHC). The goals of this study were to:

1. Understand a particular instance of AGHC – for example what happens, who does what, and the limitation and benefits of the current system;
2. Observe the environment where this is happening;
3. Understand patients’ needs and requirements regarding PHRs; and
4. Establish a working relationship with patients and AGHC staff.

4.1 Research Perspective

Research studies in areas of ICT4D focuses on development issues. The concept of “sustainability” is important to consider in any ICT4D studies in order to deliver a sustainable ICT solution. As a result, ICT4D experts advise researchers to build artefacts based on what people have, and what people can do. For instance, a mobile phone is an ICT tool that the majority of people in developing countries own. Therefore, providing an offline access of PHRs to users including patients and healthcare providers creates an opportunity for mobile PHR systems.

Additionally, the concept of “contextualisation” has also been emphasised in ICT4D studies. According to Wicander (2011), “contextualisation entails having a local problem and local resource as a starting point, having a bottom-up perspective, and considering the local communication patterns regarding information transfer”. However, most EHR systems designed for developed countries often rely on top-down approach, and advocates adoption of theoretical perspectives that are not founded on a rational and mechanistic view of the users (Benbasat & Weber, 1996).

In this study, the researchers opted for the research approach that focuses on what people do and their socially situated actions. This is important especially when taking into account the magnitude of failures when implementing healthcare solutions in developing countries, which is related to lack of knowledge and understanding about the actual context (Anokwa, 2010).

4.2 Research Design

The research approach employed in this thesis is deeply influenced by the Patient-Centred Design (PCD) paradigm. The choice of the research design is also in agreement with healthcare institutions/organisations such as the Institute of Medicine that advocates for patient-centric approach when developing healthcare technologies for patients.

4.2.1 Patient-Centered Design

Patient-Centred Design (PCD) is an approach derived from User-Centred Design. It involves patients in the decision-making and development process of an ICT solution (Frampton, Gilpin, & Charmel, 2003; Rodriguez, Casper, & Brennan, 2007; Demiris et al., 2008; Reis, Freire, Fern´andez, & Monguet, 2011). Patient-Centred Design empowers patients to have an active role in making choices and input during the design and development of an interactive health technology for patients (Dabbs et al., 2009; Demiris et al., 2008). PCD involves listening to patient's needs and requirements as well as considering the social, culture and technical context for the implementation of the system. Reis et al. (2011) documented the reported benefits of PCD: increase of the communication between the healthcare figures, end-user satisfaction, achieving expected benefits, among others. Thus PCD provides the potential of empowering patients, and supports a transition from a role in which the patient is only the passive recipient of care services to an active role in which the patient is involved in the design and decision-making process.

4.2.2 Patient-Centered Design (PCD) Processes

Pateint-centered design activities are arranged iteratively into four typical software development phase; Analysis, design, implementation and deployment. Figure 4.1 describes the activities of PCD.

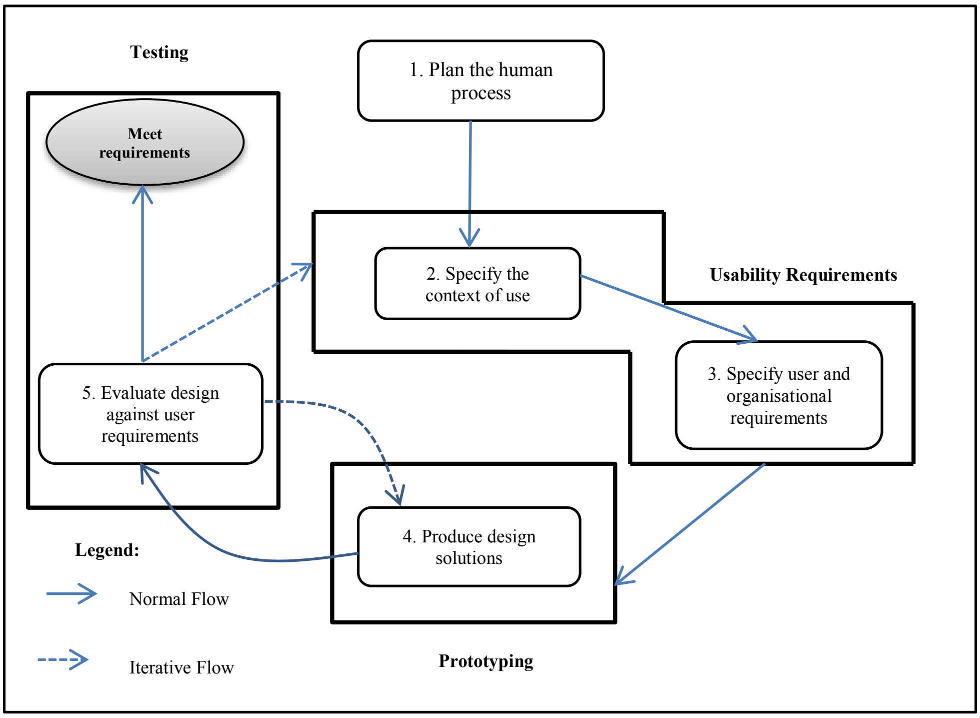

Testing
1. Plan the human process
Meet requirements
2. Specify the context of use
Usability Requirements
3. Specify user and organisational requirements
5. Evaluate design against user requirements
4. Produce design solutions
Legend:
Normal Flow
Iterative Flow
Prototyping

Figure 4.1: Patient-Centered design activities (adapted from Bevan & Curson, 1999)

Step 1: Plan the human centred process: After identifying the design needs, the designer team plans which method to use during the distinct phases of the approach. Communication among the project team and teamwork are extremely important.

Step 2: Specify the Context of use: This involves knowing the environment where the system will be used.

Step 3: Specify user and organisational requirements: This stage determines the tasks that users should accomplish when using the system. The project team define users and personnel involved using direct observation or contextual inquiry (Jones & Marsden, 2006; Dabbs et al., 2009), and/or participatory design (Greenbaum, 1993; Jones & Marsden, 2006).

Step 4: Produce design solution: In moving towards the creation of a functioning system, the design team engage users in co-design through participatory design approach (Jones & Marsden, 2006)

Step 5: Evaluate design against user requirements: Usability inspection methods, such as heuristic evaluation, user experience evaluation and focus group method evaluate the proposed designs. The idea behind this testing is to assess the degree at which requirements are achieved. Narratives and explanations of the study participants through think-aloud method or post-study open ended interviews are some of the techniques that are used to evaluate the system (Preece at al., 2002; Jones & Marsden, 2006; Lewis & Rieman, 1994).

Eason (1987) identified three types of technology users: primary users, secondary users, and tertiary users. Primary users are those persons who actually use the proposed technology. Secondary users are those who will occasionally use the technology or through an intermediary, and tertiary users are persons who will be affected by the use of the technology.

In this study, the primary and secondary users are the patients, and tertiary users are the healthcare providers. Abras et al. (2004) and Preece at al. (2002) described that secondary users can greatly be affected by the solution and thus need to be considered in the design process.

Patient-Centred Design is an approach that is accomplished through the healthcare providers and patients involved, applying some of the most well-known methods of UCD: interviews, questionnaires, focus group and participatory designs (Greenbaum, 1993). Therefore, Patient-Centred Design starts by listening to the patients and providers' needs and requirements besides considering the social and technical context (Reis et al., 2011).

4.3 Requirement Analysis, Fact-finding and Conceptualisation

The overall aim of this baseline study was to understand the current working environment of the patients and healthcare givers, prior to the introduction of the new technology. This phase of the PCD is comparable to contextual analysis in User-Centred Design (UCD) (Dabbs et al., 2009; Beyer & Holtzblatt, 1999). To ascertain how the current healthcare system works, and assess the end-user needs, we conducted a contextual inquiry with patients and healthcare providers at Allan Galpin Health Centre (AGHC). A number of studies have recently emerged which have used this approach (Dell & Borriello, 2013; Dabbs et al., 2009). Additionally, the Allan Galpin Health Centre was selected on the basis of its past and current trials of E-health systems, and the fact that it was relatively easy for the researcher to find a contact person. Therefore, the state of healthcare services and challenges through interviewing three healthcare practitioners and sixty patients from AGHC are presented.

In order to understand the process of healthcare services and the tools used to provide these services, we conducted a three-part study. Since this was an initial exploratory study, the first part involved qualitative interviews with healthcare givers to find out current practices and challenges of providing healthcare services. This approach was used because it provides in-depth understanding of phenomenon or events (Coble, Maffitt, Orland, & Kahn, 1995). The researchers completed three in-depth interviews with the healthcare practitioners. The healthcare practitioners were selected based on the fact that they had some experience with the institutional healthcare information system (Clinic Master). As described earlier, providing an offline access of PHRs to patients and healthcare providers in developing countries where majority of population owns mobile phones creates an opportunity for mobile PHR systems. Therefore, a semi-structured interview was conducted to facilitate in-depth exploration of providers' perception towards mobile phone-based PHR system. Additionally, since the researchers were trying to explore and understand the structure of PHRs, the following sample questions were included in the interviews: what constitutes patient medical records; what information goes into a personal health records and lastly, in terms of patient confidentiality, what information the patient can have on a mobile phone? The interviews were conducted at the health centre in the office of the clinical officer. The interviews were organised to take about an hour each, but in practice each interview took two-three hours. This gave the respondents an opportunity to discuss their work and relationship with the patients.

During the initial part of the interviews, the respondents were also asked to give examples of situations where they consider the current health record system unsatisfactory. These situations were then discussed in greater depth. The respondents were then asked to give concrete examples how they dealt with them.

The rapid ethnography was the second part of this study. As noted by Millen, (2000), rapid ethnography was done to understand the environment in which the system will be used, and validate the earlier findings (Fiore-Silfvast et al., 2013). We observed 22 patient visits at AGHC, out of which four were in the clinical officer's office where the clinic health information system (Clinic Master) was used. Particular attention was paid to observing the ways in which healthcare practitioners interact with their patients, how it affects their workflow, the challenges and opportunities of the current system, and the practices around the use of the patients' records. Field notes were recorded during all observations in order to maintain the richness of the data. This study generated additional data that strengthened the validity of the earlier findings, and expanded our ability to contextualize and make sense of conflicting data.

The third part of this study constituted a quantitative study with patients at Allan Galpin Health Centre. After receiving ethical approval from the National Research Council (UNCST) and the Institutional review board (Appendix 4), we recruited and interviewed 64 patients from among the patients who visit the Centre. The semi-structured interview protocol contained a combination of yes/no, and open-ended questions that determined how often the participants visit the healthcare provider, what kind of information are they always required to provide and how would they "feel" about having their personal health records on mobile phones. The coverage of the survey was based on the PHR literature review (Tang et al., 2006) and consultations with clinical officers. The respondents were made aware that their responses are voluntary and will be treated with strict confidentiality. We therefore did not need to do any advertising to recruit participants since the interviews were administered during the patients' hospital visit.

Since we were interested in general health record management problems, regardless of the format, individuals who viewed their paper or electronic health records within the past six months were eligible to participate in the study. Participants were recruited between December 5th 2011 and February 7th 2012, and a convenience sample of 60 unpaid volunteers completed the survey. The four patients that did not complete the interview were because of poor health (understandably) at the time of the survey. The one-on-one contact by the researcher with patients took place at AGHC premises. The study was in general well received and all the patients approached agreed to participate in the study.

4.3.1 Data Analysis

Our non-concurrent studies generated two types of data: quantitative responses and qualitative data resulted from semi-structured interviews with healthcare providers. The quantitative data necessitated the creation of a codebook in order to convert responses into numerical form. The numerical data was then entered and analysed using statistical package for social scientists software in order to generate descriptive information described in the results section.

Likewise, the qualitative data was analysed systematically, subjecting it to a three-stage analysis methods: data reduction, data display and conclusion drawing (Pope, Ziebland, & Mays, 2000).

4.4 Results and Implications

In the next section, we present results from our studies; in particular, we reveal how the current healthcare system works, the challenges and describe the perception of patients and healthcare practitioners towards mobile phone-based PHR systems.

4.4.1 Environment Description

Allan Galpin Health Centre (AGHC) is a Uganda Christian University health centre responsible for the provision of healthcare services to students and staff (and their dependents). The clinic is located within Uganda Christian University Mukono, along Bishop Tucker road, about 33 kilometres from Uganda's capital and main city Kampala. Currently, the Allan Galpin Health Centre (AGHC) offers health-related services to over 8000 people.

Our preliminary studies reveal that although AGHC installed healthcare information system to provide efficient healthcare services, the process of using patient data is still paper-based. When the healthcare givers see the patients, they complete paper forms that document the encounter. These forms are eventually added to a paper record in order to support offline access i.e. when Clinic Master is offline due to frequent power outages and/or unreliable Internet connections. Every few days, the encounter along with the laboratory results is manually entered into Clinic Master. Upon a return visit, majority of healthcare givers review the patients' records on paper using past encounter to guide decision making.

4.4.2 Healthcare Challenges

During our time working with the Allan Galpin Health Centre, we observed two common and persistent challenges that hinder the health centre to attain its goals: 1) fragmented paper-based patients' information and 2) unprotected patients' records. These issues were common in all departments that we visited regardless of the size. In the next section, we describe the challenges, and present possible solution that can address these challenges.

Challenge 1: Patients' Health Records are not Well Protected

During the course of a seven-month period at Allan Galpin Health Centre, we had an opportunity to go through Clinic Master and observed that, despite the high level of regulations and laws surrounding EHRs use and protection, Clinic Master does not adequately provide meaningful access control mechanisms to patients' records. Records on the server are not protected, and all clinic employees have access to the medical records for all patients. The server only relies on a computer audit application to investigate the security problems after the act. Considering other healthcare institutions that we visited during the course of this study in Uganda, we observed that these challenges were common in all institutions regardless of the size and location.

Challenge 2: Fragmented Paper-Based Patients' Information

Although Clinic Master has greatly improved service delivery at the Allan Galpin Health Centre, its operations are fully dependant on power and stable Internet connections. When the server becomes unavailable due to frequent power outages in Uganda (during this period, the country was going through 12 hour rolling power cuts), it becomes impossible to reach patient's records. Under certain circumstances, this could result in patient harm. The clinical officer indicated that;

"……..within this week, we have experienced Internet interruptions twice whole days, and 12 hours per day load shedding……"

When asked how they have been dealing with such situations, the respondents reported that such problematic situations have forced them to keep paper-based files for patients (Figure 4.1), which represents a massive fragmentation of clinical information. She further noted that other health centres have embarked on giving patients their records (paper-based records) after treatment such that, every time a patient visits the centre, he/she presents this chart to the healthcare professional, showing their medical history.

Based on these observations, it is clear that personal devices such as mobile phones can positively affect the way health records are stored and shared. A survey conducted by Mercy Corps (2012) demonstrated that 65 percent of households in Uganda own cellular handsets while 90 percent have access to cellular services (Kyla, 2013). The motivation for using cellular handsets is clear evident that mobile phone-based PHR system can be deployed to a large percentage of the population in Uganda.

4.5 Perceptions and Views towards Mobile Phone-Based PHR

The baseline expectations of healthcare practitioners towards mobile phone-based PHR were overall positive, although two practitioners had some concerns. All the practitioners agreed that the care of patients would be improved if patients own their medical records on mobile phones. Table 4.1 summaries the types of information that healthcare practitioners felt that they and/or their patients should have access to within the PHR.

Table 4-1: Clinical officer's perspective on who should have access to information

Information	Doctors' group	Patient
Demography data	√	√
Discharge summary	√	√
Major surgeries	√	
Lab test results	√	√
Medication	√	√
X-ray results	√	
Allergy	√	√
Chronic problems	√	√
Immunisation	√	√
Emergency Information		
Doctor's name and phone number		
Next of Kin name and phone number		
Blood group		
Allergies		

Additionally, the practitioners also highlighted some of the information a patient can have on a mobile phone as;

1. Demographic information
2. Clinical problems
3. Previous lab test results
4. Diagnosis
5. Previous Medication
6. Allergies
7. Chronic Problems and
8. Immunisation plus others depending on the healthcare professional

4.6 Healthcare Practitioners Concerns

Across the three healthcare practitioners who participated in the interview, two expressed concern that the confidentiality of patients could be violated if patients' health records are stored on mobile phone. In particular, a clinical officer stated that some of her patients did not always reveal their entire medical history to all other nurses and clinical officers.

Additionally, a doctor expressed concerns about the possible misinterpretation of medical information and comments in the medical notes if patients were able to review their own records. In one response, the clinical officer advised that information accessed by patients needs to be customised to minimise medical terminologies and misinterpretation of medical comments. All the healthcare practitioners interviewed highlighted that mobile phone-based records should be password/PIN protected to minimise violations of patients' confidentiality and privacy.

One clinical officer further noted that when we empower patients to have their records on a mobile phone, issues such as self-treatment may arise. This is one of the major problems that should be avoided. When asked how is this possible, the clinical officer explained that once patients have health information such as previous medication on their mobile phone and they know such medication helped them with the previous illnesses, they are likely not to come back for diagnosis and proper medication. They may prefer to visit any nearby pharmacy and buy the previous medication. However, she further recommended that the Government should put in place a law that binds pharmacies from selling drugs to patients without proper prescription from the doctors.

Furthermore, one health practitioner also highlighted that patients' emergency information in the PHR tool need to be protected and at the same time accessible when needed by healthcare professional. For instance, if the patient requires an emergency attention, then the medical staff should be in position to identify and obtain the emergency key in order to prevent unintentional death to the patient.

4.7 Patient Survey Results

This section presents both qualitative and quantitative results from the semi-structured interviews with patients at AGHC. Table 4.2 below describes the demographics of the participants. The table demonstrates that the selected sample was comprised of individuals with low literacy level.

Table 4-2: Sample's demographics

Nos.	Characteristics	Sample distribution
1	Gender	Male: 36 Female: 24

2	Education	Primary: 7 High School: 21 Tertiary: 32
3	Age	Less 20: 22 20 - 29: 17 30 – 39: 11 40 – 49: 09 50 and above: 01

Of the 60 subjects who participated in the study, 81.67% visit the healthcare facility only when they are sick, 6.67% at least once a year, 8.33% once in six month and 3.33% once a month. Figure 4.2 shows the results.

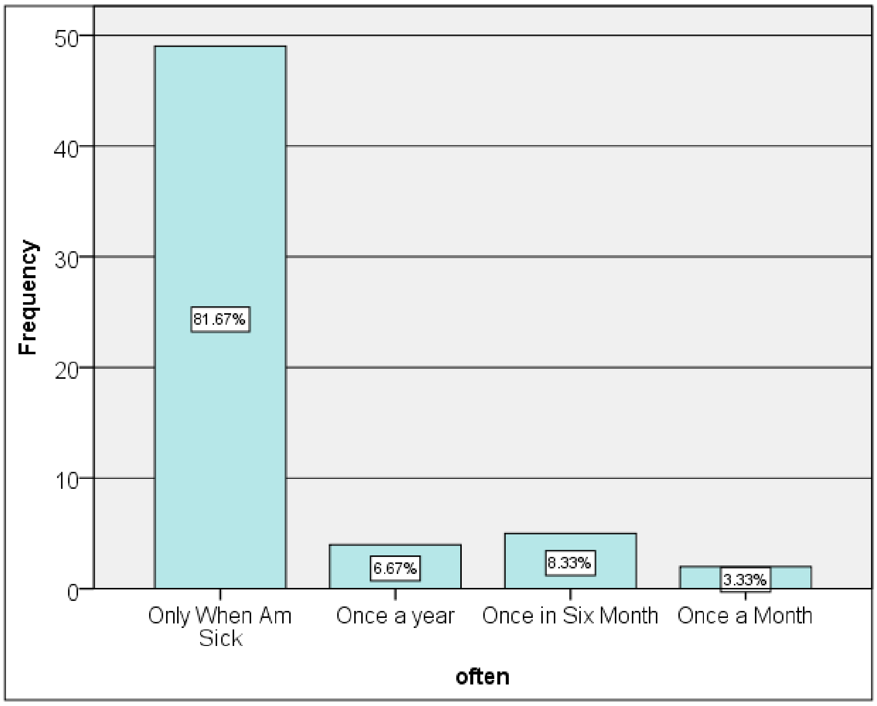


Figure 4.2: How often do respondents visit the health service provider

Two-thirds of the patients (66.7%) noted that they had seen some portion of their health records (mostly laboratory results and medications), and 83% believed that a personal health record would help them manage their personal healthcare. The most common reasons why participants would like to access their records were to enhance their understanding of their medical condition, ensure that their records are accurate and up to-date, and manage their care at home.

Participants were further asked when they visit the health service provider, what kind of information the doctor always required to provide. Table 4.3 below gives patients responses.

Table 4-3: Information Doctors Typically Request from patients

1	Demography
2	The major health problem and its time course (e.g. headache for past 4 hours).
3	History of the present illness
4	Symptoms
5	Medication taken
6	Allergies
7	Chronic problems
8	Immunisation – (option)

Although 8% of our respondents say the service provider does not collect personal information, 92% of the respondents provide personal information to the health service provider. Participants were also asked how they would “feel” if their medical records are shared across different health service providers such that they don’t have to explain themselves every time they visit a different provider. Only 2 patients were comfortable with it and 58 were much concerned with the privacy and security of their records. 87% noted that they would feel comfortable and secure to be in charge of their records, 6% said they prefer health service providers to be in charge since they have not received any problem with it and 7% did not given any response.

Of the 92% who provide personal information to the health service provider, 88.3% prefer to keep and manage their own medical records and only 11.7% want their health service providers to be in charge of their records because they are so forgetful and fear that they may lose them. Interestingly, when they were asked whether they are willing to use their personal device in storing and sharing their medical records, all respondent gave a positive response and highlighted that it would be better to have their health records on mobile phones the way they move with their money using mobile money applications.

The survey questions also asked participants about the number of times they had viewed their records in the past year; the number of facilities from which the records were requested; the records' format and the time spent on the last view. 62% percent of the respondents highlighted that they would like to view their records if they are given an opportunity to do so; 4% viewed their records only once in the past year, 7% viewed them between two and five times; 11% – more than five times; 16% – following each visit. The majority of the participants had viewed their records from more than one health facility. Handwritten paper-based records were the most frequently viewed format (82% of participants) followed by typed paper records (18%). The mean amount of time spent per record review was 30 minutes with standard deviation equals to 29.

When asked if they receive enough information about their condition upon discharge from the healthcare facility, 83% of participants believe that they don't receive enough information and 17% felt that they receive enough information. The majority of the participants wanted more information about necessary follow-up care and managing their care at home.

The information seeking behaviour questions asked participants to tally the reasons for looking at their records, specific information they wanted to find, and the sections they viewed. The responses were recorded for each of the three questions. Table 4.4 and 4.5 presents participants' reasons for requesting their records, and the specific information desired respectively. The most frequently viewed parts of the records included lab test results (88%), medication information (history and current) (81%), doctors' prescription/notes (62%) and contact information (specialists and emergency contacts) (56%), and all the participants felt that the inclusion of allergy history is necessary in the personal health record. The preferred format of this information is paper format although some participants endorsed some type of electronic format. Further explanation for the preference of paper format indicated the familiarity with hardcopies, which allows patients to conceptualise what their health information might look like on paper. Seventy-eight percent of the respondents highlighted that it is very difficult for them to conceptualise how their personal health information can be presented and navigated in an electronic format.

Table 4-4: Reasons for Accessing Records (N = 60)

Nos.	Reasons for accessing Records	Percentage
1	Enhance their understanding of their medical condition	83%
2	Ensure that the information is available to the doctor whenever they visit the healthcare facility	78%
2	Important in case of an emergency	69%
3	Have a detailed information about my health	86%
4	Take more active role managing own health	83%
5	Confirm record's accuracy	51%
6	Explain situations to someone else	38
7	Check negative comments	11%
8	Check if best possible care was given	6%

Table 4-5: Specific information desired (N = 60)

Nos.	Reasons for accessing Records	Percentage
1	Lab test results	88%
2	Medication	81%
2	Details of diagnosis	62%

3	Contact information	56%
4	Chronic problem	24%
5	Immunisation information	76%
6	Allergies	100%

The survey questions also asked participants which type of device they prefer in storing and managing their health records. 91.6% said they prefer mobile phones because they are affordable and portable; 6.7% prefer laptop devices because of bigger screen size for records display and one respondent prefers PDA because he had got one.

Furthermore, participants were asked whether they have any idea about keeping "stuff" private on the mobile phone. Of the 60 respondents, 88.3% said yes and 11.7% said no. Of the 88.3% who said yes, 76.6% explained that they had used PIN for applications like mobile money, M-banking and phone locking/unlocking, 5% said, they have used username and password for only emails and 18.3% said they have used both PIN and username/password to protect their personal data.

4.8 Interpretation and Discussion of results

This section presents the discussion and interpretations of patient's needs and experiences with personal health records, which provide insights for optimal "patient-friendly" PHR design. The following four key points were emerged from the survey.

4.8.1 Personal health records can be a valuable resource for enabling patient's participation in their healthcare.

The results from the survey demonstrate a desire for patients to have access to personal health information. A patient's interest in their records shows the desire to play an active and collaborative role in medical decision-making. Patients are more likely to view their records in order to enhance their understanding of their medical condition, and take a more active role in managing their own health. The survey further reveals that for many patients, viewing their records translates into care-related decisions and actions. However, gaining access to the records is often a challenge.

4.8.2 Privacy and security issues

From the data analysis described above, there is a significant number of patients who provide personal information to their health service providers. Most of the patients whose personal information is collected would mind if their information is accessed by unauthorised users. Although the majority of patients would like to have their records on mobile phone for portability, personal management and control, they are also concerned about cases of mobile phone theft that may lead to unauthorised access of their health records. In addition, some patients pointed out that the disappearance of their mobile phone with their records either through theft or misplacement may lead to total loss of their health records.

Mandl et al. (2001) deduced that patients' electronic health records should be stored and exchanged according to public standards and that the patients should have control of access of their health records. International health systems standards such as HIPAA[13] and HL7[14] dictate that patients should be able to define explicit authorization with an expiry period and should be able to get accountability for all the access. The analysed data from the patient interviews reveals that the patients have the same requirements as specified by Mandl et al. (2001) and the international health systems standards.

4.8.3 Professional language the barrier to record comprehension

The study participants provided narrative comments about barriers towards record review, and heighted professional language (medical terminologies) as the major barrier. Understanding the records is not easy. Patients who reviewed lab test results and the doctors' notes found the records difficult to understand. The need to provide terminology support was often expressed by the majority of participants. Preference for "simpler words" or "layman's terms" to replace medical terms was highly noted by the participants in order to provide a user-friendly system.

4.8.4 Carefully designed PHR systems can address professional language barrier

The study demonstrates that the majority of patients view their records in a paper format. This provides limited opportunity for comprehension support and portability. Additionally, literature reveals that patients prefer paper versions (versus electronic) of their records because of concerns regarding security of their records (Leonard, 2004). However, Hassol et al. (2004)

[13] **http://www.hhs.gov/ocr/privacy/**
[14] ***www.hl7.org***

and Avancha et al. (2012) explain that electronic PHRs can ease record access, support secure sharing of PHRs, and eliminate the problem indecipherable handwriting. Similarly, Fridsma, Ford and Altman (1994) described that electronic PHR system can provide terminology support that enable patients view and understand their records.

4.9 Summary

In this chapter, we have presented some of patients' requirements that lead to the design of a mobile phone-based PHR system. Through interviews and observations, we have established a better understanding of patients' needs and preferences.

One consistent observation we found during this study was lack of practiced knowledge about electronic personal health records. Patients were more exposed to paper-based PHR systems. Moreover, current PHR practices and services are primarily paper-based. Paper-based PHR processes impose many disadvantages such as incorrect recording of diagnoses, unavailability and loss of patient information, delays in accessing the information and space limitations for record-keeping. Somehow, we need to automate these processes in order to minimise some of these difficulties. In the next chapter, we describe how patients were involved in automating these processes in order to address their requirements.

"It is not the healthy who need a doctor,

but the sick"

- *Matthew 9:12*

CHAPTER FIVE: MOBILE PHONE-BASED PHR SYSTEM: CONCEPTUAL AND PARTICIPATORY DESIGNS

5. Introduction

In this chapter, we discuss how a mobile phone-based PHR system was design from a basic paper prototype to a high-fidelity prototype called the M-Health App system. As has been described in chapter four, this part of the design process required us to design an interactive system that enable patients to securely share their health records with the medical practitioners. Therefore, a participatory design approach was used, in combination with Human Access Points (HAP) technique (Marsden, Maunder, & Parker, 2008) that supports the use of a person in the community who is more knowledgeable about the potential of the technology to design the system. In the next section, we describe the usefulness of participatory design and Human Access Points towards the design of M-Health App system.

5.1 Participatory design

Participatory design (PD) is an approach that was adopted from the Scandinavian approach of workplace in decision making. In PD, the end-users that are intended to benefit from the system play a critical role in designing the system. Participatory approach to design forms part of Patient-Centred Design (PCD) (Tran, Zhang, Stolyar, & Lober, 2005; Rodriguez et al., 2007). It departs from the idea of top-bottom approach that advocates for greater use of theoretical perspectives that are not founded on a rational and mechanistic view of the end-users. PD views the design process within the context of the user's environment, and considers the attitude and perceptions of the end-users towards the technology, and their interaction with each other in the design process (Gitau, 2012). Therefore, PD makes end-users equally accountable for the design decisions made about the system.

However, critics of the participatory design method have questioned the merits of treating end-users as equal partners in the design process. For example, Scaife and Rogers (1999) argued that end-users do not know enough to be equal partners, and they can only be informants in the design process. Similarly, Young and Chang (1997) described that asking end-users what information they would like to receive is not efficacious due to the fact that users are normally not well versed in "system operations"; what end-users are very good at is identifying the functionalities they would like to have at the moment they are experiencing system.

To bridge this gap, Marsden, Maunder, and Parker (2008) proposed a technique that makes use of Human Access Points (HAP). The technique allows a person in the community who is more knowledgeable about the potential of the technology to act as a proxy for the community in the design process (Figure 5.1). It relies on the assumption that the HAP is actually interested in the design process, has the ability to participate, has knowledge of the envisioned technology, and is actually available to participate. Additionally, HAP technique also assumed that the HAP can articulate the needs such that the system being built will address those needs (Gitau, 2012).

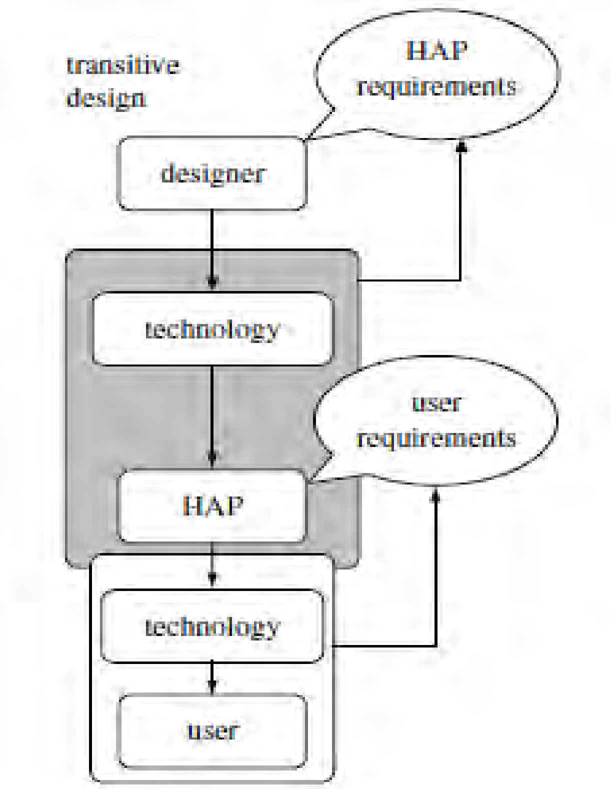


Figure 5.1: Human Access Points. Adopted from Marsden et al. (2008)

In the context of this thesis, the Human Access Points (HAP) was chosen for the following reasons: as described in chapter four, the key characteristics of the majority of patients receiving treatment at AGHC are digital illiteracy, have insufficient education and even lack access to electronic PHRs. As a result, we needed to use Human Access Points in the design of M-Health App system.

5.2 Design Process

This section presents the design phases of M-Heath App System. After three months of being at Allan Galpin Health Centre (AGHC), and analysing the data collected, we noted three themes that could inform the design of a possible interactive PHR system. The three themes were: design for handset users; design for offline access of PHRs; and design for low literacy users. These themes informed the structure, flow and interactiveness of M-Health App system. Gitau (2012) described that in HCI, it is a standard practice to synthesize the data collected from end-users to come up with a list of themes that a design must fulfil. Using this approach, user needs were captured and generated a list of system requirements.

Therefore, from the observations and interviews conducted and described in chapter four, the first three design decisions for M-Health App become apparent. These are;

1. Design a technology that overcomes the challenges of paper-based personal health records, and support secure sharing of PHRs.
2. Develop a mobile PHR technology that minimise professional language barrier to patients and support patients participate in their healthcare.
3. Provide a tool that protects patients' privacy within their context of use.

In the next section, we describe how these themes were translated into a usable M-Health App system.

5.3 Recruiting Representative Human Access Points (HAP) for M-Health App Designs

Recruiting representative patients was one of the challenges we faced during this phase of development. Patients at Allan Galpin Health Centre (AGHC) come to the facility, get treatment and leave. Tracing these patients at their home and/or place of work was very difficult, since majority of the population move by necessity rather than choice, with no orderly and lawful migratory channels available. A total of 12 patients who get healthcare services at AGHC were recruited to participate in the design process. This number was considered ideal because industrial environments normally use seven participants and more during participatory design sessions (Boehner et al., 2007). The participants were randomly but purposely recruited to take part in the design process. They were mainly students who were earlier participated in the design of Clinic Master, and thus familiar with the digital technology. Therefore, they were used for design ideas and initial testing of the prototypes. Three of the subjects had participated in our earlier formal interviews. Figure 5.2 below shows one of our sample interactions with patients.

Figure 5.2: An interaction with patients

A week after recruitment, we invited the participants to attend the Allan Galpin Health Clinic and eight of the twelve appeared. They were briefed about our research project and agreed for the next meeting. All participants were offered Ushs. 5000 (about $2) as compensation in form of transport.

5.4 Simple Technology Artifacts

There are a number of approaches that have been used to inspire participation of users in the design of a new technology. Among the approaches is to introduce a simple technology artefact whose capability is obvious and present it to users at the early stage of the design process (Ramachandran, Kam, Chiu, Canny, & Frankel, 2007). This approach stimulates ideas from end-users and creates a platform where users envisage the use of the technology within the context of their daily life and contribute easily to the design process.

In this study, we started by designing technology artefacts. These artefacts were phone-based PHR prototypes that intended to motivate participants and get better understanding of the operations performed, and also assess users' reactions to the prototype.

Every morning of the first three-days we visited the health centre, we were provided with the meeting room, chairs, and notified that the room is free for the study the whole day. The clinical officer helped to organise the patients, and introduced the researcher to the patients before the main session begins. We often sat in chairs (see Figure 5.3) in the centre of a large circle in order to avoid mixed and an equal exchange of ideas.

Participants were briefed about the overall objectives of the session and the goal to be accomplished. Initially, three quarters of the participants were very confused about what we were showing them. But when we explained a little more about what we were doing and the purpose of the project, things became a lot clearer as demonstrated by the following participant;

"……… From mobile money to mobile medicine, this is exciting……….. "

This statement excited most of the participants and two of the patients noted that, at last, someone is developing a system for them.

Figure 5.3: Design session

Interesting to note was that the majority of the participants were able to understand the benefits of the study. Most of the participants easily identified PHR content, its purpose, as well as other system functionalities. These results encouraged us to continue the design process.

Two participatory design sessions were conducted at the meeting room, faculty of science and technology, Uganda Christian University. Eight participants were divided into two groups, each with four participants in which the researcher acted as the facilitator for each group. Figure 5.4 below shows an example from our PD sessions. Participants were reminded that they were the users of the mobile application and that is why they were developing the application. They were also asked to think about the things that they do frequently during and after visiting the doctor or any healthcare professional. Participants were also asked to prioritise this information/activities although the clinical officer highlighted that all the information requested from patients are of equal importance.

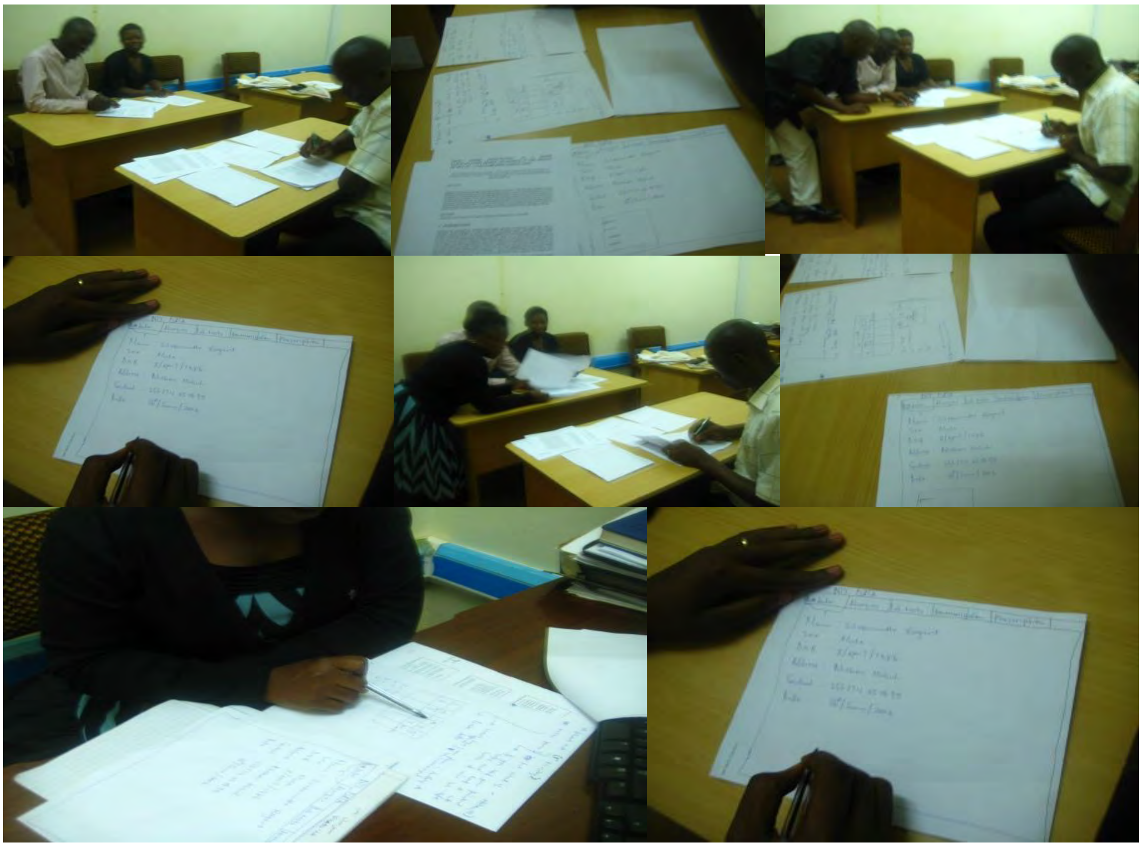


Figure 5.4: A Few Examples from our PD sessions

An introduction to paper prototyping technique was given and the following aspects were explained to the participants as proposed by Snyder (2003);

1. Introduction of paper prototyping, its history, relevancy and how it relates to participatory design
2. Participants were also informed that there is no right or wrong answer during paper prototyping and they are free to show their creative side
3. Participants were briefed and provided stationery and materials used to develop paper prototypes. Samples of paper prototypes were shown to them in order to stimulate their designs

4. The benefits of paper prototyping were highlighted throughout the session in order to encourage participants give full commitments

The two groups worked separately in the development of the prototypes. At the end of the sessions, a number of requirements were produced. All members in each group developed the prototypes collaboratively.

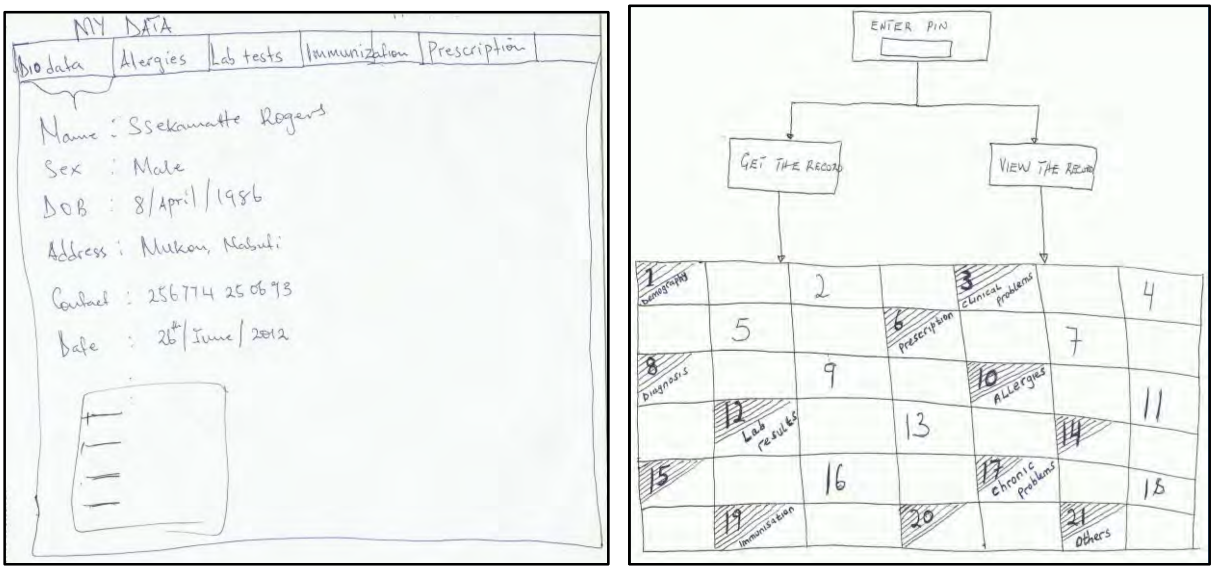
Participant were then presented to the story-boards showing activities that stimulated the production of the paper-based M-health Application design. They were requested to re-arrange them starting with what they would want to see first. After each session, a walk through was done in order to identify any issues and for participants to justify their choices. Each group then started developing the prototypes with the researcher as the facilitator.

5.5 Evaluation – The Paper Prototypes

At this stage, our goal was not to come up with a complete design but to gather more requirements through paper prototyping. Each participant provided one to two incomplete screens and several issues were identified by the facilitator with the prototypes; incomplete interfaces and reluctance from two of the participants to sketch the interfaces. Simplicity towards the interface/screen designs was the first observation noted by the facilitator. In order to harmonise all the functionalities that appeared on the screens, there was a need to strike a balance between these functionalities and the number of steps needed to accomplish the needed task. Participants agreed about what the patients need in order to view and share their records;

1. Locate the application from the website and then download it to the mobile phone
2. Install the application to the mobile phone
3. Download the records using your PIN
4. View and share the records with the healthcare professional.

Figures 5.5 (a) and Figure 5.5 (b) below illustrates two samples of paper prototypes that were created by the participants. Through 5 (five) iterations, and consultation with AGHC clinical officer, we came up with a set of three paper screen elements. We then transformed these screen elements into the digital screen captures, using Java. The screen shots of the initial high-fidelity prototype can be found in Appendix 4.3.



Name : Ssekamatte Rogers
Sex : Male
DOB : 8/April/1986
Address : Mukon, Nabuti
Contact : 256774 250693
Date : 26th/June/2012

(a) **(b)**

Figures 5.5 (a) and (b): Sample paper prototype screen elements

The features of M-Health App prototype at this point could be summarized as follows;

- **Download Records feature**: Enables patient to download their records from the hospital server to the mobile phone
- **View Records feature**: Permits patients to view their health records.

Figure 5.6 gives a system overview of M-Health App architecture in its initial stages. The architecture comprises a mobile application interface to the server, running an apache web server and storing health records on MySQL database. Furthermore, it also interacts with a web server that is maintained by the hospital. The web server supports read access to a patient's health records. Patients are authenticated via Personal Identification Number (PIN) to the web service to retrieve their health records. Once the records are downloaded to the mobile phone, the M-Health App system breaks down the records into an XML structure such that records are viewed selectively.

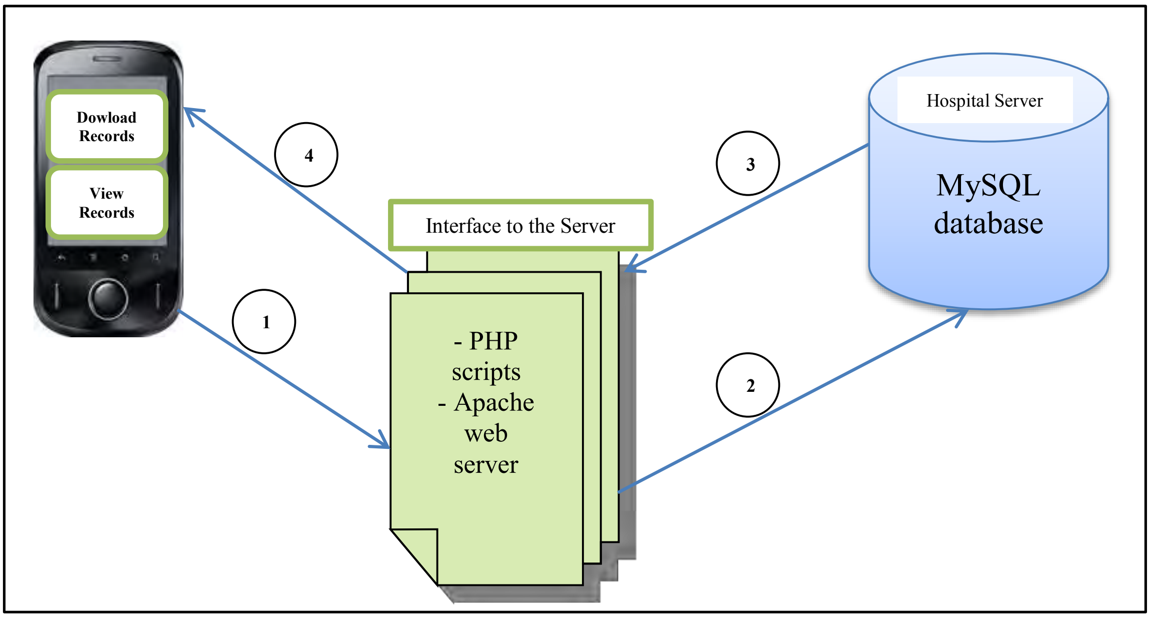


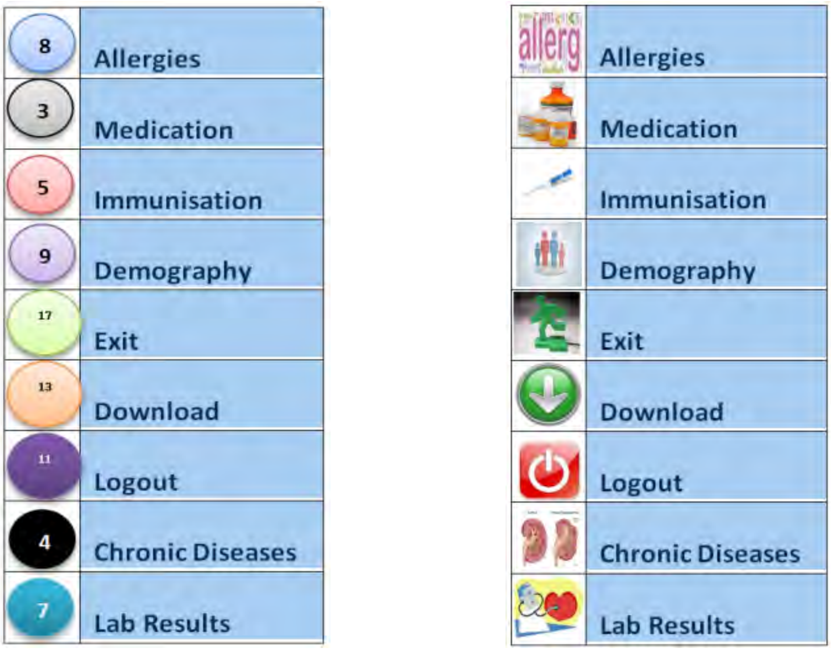
Figure 5.6: M-Health App system overview

Contrary to the previous approaches, our architecture enables patients to download and update their PHRs onto the mobile phone, and share their records with healthcare providers in an offline mode i.e. when hospital servers are offline due to unstable main electricity and/or unreliable Internet connection.

5.5.1 Navigation and Associations

During the design and evaluation of paper prototyes, we observed that navigation functions (for selecting individual items) were associated with numbers and picture/image. The idea was to represent navigational paths in the interface. For example, some participants were trying to navigate the prototype using numeric "shortcut" while other particiapants used images.

In order to use numbers or images as navigational aids in our application, we had to ensure that end-users are able to associate them with the actions. To test this, we conducted an informal test with the HAP where participants were given prototypes to memorise associations between identifers (number/images) with actions. Figure 5.7 (a) and Figure 5.7 (b) describes the prototypes, showing associations of identifiers with actions. The identifiers were selected from a set of numbers and a variety of images (Parikh, 2007).



(a) (b)

Figure 5.7: Prototypes showing Numeric and Image Identifiers

The test were conducetd by showing users a sequence of images or a set of numbers that are associated with a respresentation of an action or idea. Particpants were then given as much time as they needed to memorise the relationships (Parikh, 2007). After the lapse of the agreed time, participants were asked to recall the images or concepts that were associated with particular identifiers.

At the end of the study, we observed that numeric "shortcuts" such as numbers were very difficult for participants to remember and narrate. Three quarters of the particpants had difficulty in remembering and associating the concept with a number that is meant to represent. However, we noted that participants were much successful in associating the action with an image that could be visually related to the idea meant to represent. This observation presented the idea of using images in M-Health App system.

5.6 Formative Evaluation

According to Rogers, Sharp and Preece (2011), formative evaluations are done during the design process to check that the system continues to meet user's needs. It covers a broad range of design process, right from the development of the early sketches and prototypes through to perfecting an almost finished system.

To ensure that M-Health App system indeed fulfils its purpose, we needed to test its functionality and features with a wider range of users with different characteristics. Up to this point, following the path of Human Access Points approach (Marsden et al., 2008), we had been interacting with students (those that had visited AGHC for treatment) and relying on their expertise. Therefore, it is imperative to allow the system to be evaluated through engagement with other users/beneficiaries.

The evaluation objective was to provide a deeper understanding of the end-users, the effects and outcomes of their interaction with M-Health App system, and how this could in turn inform the design, in terms of modifying the original requirements. In other words, we wanted to determine;

1. **M-Health App system Interaction:** Did users understand the system? Did the design process capture user needs correctly? Are the need and requirements represented well in the system?
2. **M-Health App system functionalities:** Does it work as it should be?
3. **M-Health App system Learnability:** Given the low and semi-literate users, how fast could they learn to use the system on their own? Was it intuitive?

5.6.1 Evaluation of Participants

To answer the questions described above, we needed to test the system with two sets of actual users: a group of patient-users; and AGHC employees. To get the healthcare practitioners' point of view, we evaluated M-Health App system to ensure that it captures and displays the correct information for their needs. We also wanted to get feedback on the format of the personal health records displayed by the system.

For the second round of evaluation, we started by recruiting seven patients, five male and two female from the Allan Galpin Health Centre who individually acted as end-users. The reason for individual sessions is attributed to the fact that patients visit the clinic at different times. Our sample size was based on the previous study conducted by Dabbs et al. (2009). The participants were then given an introductory briefing about the high-fidelity prototype, user goals and the requirements derived from our PD sessions. We tested the prototype on Huawei *IDEOS* phones, running Android OS, with 256MB of RAM. The IDEOS phones in particular were chosen as they were designed specifically for developing countries. The evaluation was driven by the following scenario: *Assume you are Cliff - a patient at Allan Galpin Health*

Centre. Cliff's electronic medical records are stored on the clinic's database server. Cliff is now required to get a copy of his records from the hospital server to his mobile phone and then selectively share them with the healthcare professional using his pin as ucu242. Please spend the next few minutes using the M-Health App system.

The participants were also given a debriefing questionnaire in order to capture their experiences with the interface. We also used an audio recorder to capture the think-loud interaction and interface usage (Nielsen, 1994b; Als, Jensen, & Skov, 2005). The analysis of the data was divided into Likert-type responses and the narrative.

According to Clason and Dormody (1994), Likert-type items is the form of the original Likert (Likert, 1932) response alternatives that are considered and analysed as individual questions. Studies conducted by Lee and Grice, 2004, Tsai et al. 2007, and Dabbs et al. 2009 have used this technique to collect information about the perceptions on user's satisfaction (ease of use), learning effectiveness and also to identify any usability issues in the healthcare technology.

Similarly, Likert-type questions with four response alternatives (strongly agree, agree, disagree and strongly disagree) were applied to determine the usefulness of M-Health App features, assess the patients' level of acceptance of the application as well as to evaluate the learning effectiveness of the application. The questions asked were based on the Dabbs et al. (2009) study for the usability of interactive health technologies for patients. A number of issues were highlighted as described in our next subsection.

5.6.2 Patient's Satisfaction

Table 5.1 describes patients' perceptions on ease of use of the M-Health App system. The table demonstrates that 71.4% (5) of our respondents thought that the interfaces can be used without thinking; i.e. it is intuitive, and 28.6% (2) indicated that the application is confusing due to the fact that some icons do not relate the functions. We further explored other opportunities for icons that can represent the M-health functions and patients suggested a number of icons.

Of the six subjects that participated in the study, 80% (4) noted that the prototype features can be explored using trial and error, and also that performing tasks are straight forward, and only one subject did not understand what "download" meant. As such, she needed some clarification. Overall, all the participants agreed that the sequence of screens is not confusing. This, therefore, confirms that the majority of participants found the prototype easy to navigate, enjoyable and easy to use.

SD – **Strongly Disagree**, D – **Disagree**, A – **Agree** and SA – **Strongly Agree**

Table 5-1: Patient's Satisfaction

Patient's Satisfaction	**SA**	**A**	**D**	**SD**
M-Health App can be used without thinking		71.4%	28.6%	
Terminologies related to the task is not understandable		14.3%	85.7%	
The sequence of screens are confusing			100%	
Performing tasks are not straight forward		14.3%	85.7%	
M-Health App Icons does not relate to the functions		14.3%	71.4%	14.3%
You can explore M-Health App features using Trial and Error		71.4%	28.6%	

5.6.3 Learning Effectiveness

The evaluation of perceived learning effectiveness of the M-Health App gives satisfactory results. Table 5.2 describes the results. The results confirm that users found the high-fidelity prototype easy to learn, navigable, enjoyable and easy to learn after training. However, two respondents indicated that;

……. navigating the application need to be improved such that the tool provides meaningful alerts. For example, when downloading the records, the application should tell the user that it is downloading.……

Table 5-2: Learning effectiveness

Learning Effectiveness	**SA**	**A**	**D**	**SD**
M-Health App is easy to use	14.3%	57.1%	28.6%	
It is not easy to navigate M-Health App		14.3%	57.1%	28.6%
M-Health App is enjoyable to use		71.4%	28.6%	
M-Health App is easy to learn after training	42.9%	57.1%		

5.6.4 Perceived Benefits

Table 5.3 describes patients' perceptions on the benefits and ease of use of M-Health App system. The table reveals that majority of respondents (85.7%) gave positive results about our high-fidelity prototype.

Table 5-3: Perceived Benefits

Perceived Benefits	SA	A	D	SD
M-Health App may make sharing my medical records easier	14.3%	85.7%		
M-Health App functions facilitates the easy with which my records can be shared		100%		
It is easy to understand the features provided by M-Health App		85.7%	14.3%	

Therefore, the positive results of the formative evaluation re-affirm that Human Access Points (HAP) can be used for design ideas and initial testing of the prototype. However, a number of suggestions for improving the prototype and introducing new services were pointed out. A compilation of these suggestions follows and will certainly be taken into account in our next version of the prototype. The next section outlines participants' suggestions and concerns about the prototype.

Feedback

- Three of the users suggested that the navigation needed to be improved such that the tool provides meaningful alerts. For example, when downloading the records, the application should tell the user that it is downloading.

Terminology

- One respondent did not understand what "download" meant. She needed clarification on some of the terms. She preferred GET RECORDS instead of download.
- She also suggested that the tool would be user-friendly if it is translated into local language

Functionality

- A need to know when records were last downloaded was also highlighted by 2 respondents.

The tool was also given to the clinical officer for evaluation and various comments were recorded;

- The clinical officer also suggested an addition of emergency function to include patient's emergency information that may be important during emergency situations.

- Information on previous medication should include dates showing when such medications were taken.

These suggestions were used to improve the prototype as described in the proceeding chapters.

5.7 Summary

In this chapter, we have presented some of our initial experiences in designing mobile phone-based PHR system for patients in rural Uganda. Based on ideas presented by the Human Access Points (HAP) during the co-design sessions, paper prototypes of M-Health App system were generated and validated to produce a final low-fidelity prototype. The low-fidelity paper prototype was the transformed into a functional prototype that was evaluated by the final beneficiaries. The results of the evaluation re-affirm that HAP can bridge the illiterate gap in the design process by using a third party from the community who understands the potential benefits of the technology to articulate end-user needs and requirements on behalf of the final beneficiaries.

After formative evaluation with the beneficiaries of the technology, we identified three major components of M-Health App system in order to achieve end-user requirements and needs;

1. Authentication component – authenticates users to download and view their records
2. Mobile application interface component – Interacts with the web server maintained by the health centre.
3. Security component – provides security of patient's records stored on mobile phone.
4. Storage component – Stores downloaded records to the mobile phone.

These components interact with each other in order to support patients securely maintain their health records on the mobile phone.

In the next chapter, based on these components and patients' needs identified during the conceptual inquiry study, we present an access control framework that protects personal health information on mobile phone.

"Predictions are always perilous;
the best way to predict the future is to create it"
- *Peter Drucker*

CHAPTER SIX: AN ACCESS CONTROL FRAMEWORK (ACOF) FOR PROTECTING MOBILE HEALTH RECORDS - A CASE OF DEVELOPING COUNTRIES

6. Introduction

This chapter picks up from chapter five – conceptual and participatory designs. In this chapter, we present the design of ACOF based on end-users' requirements, mobile phone-based PHR components, and technology gaps identified in chapter two. The chapter describes the interaction of ACOF modules, and the implementation of the PHR system called M-Health App system to support offline access of personal health records. Thus, the chapter makes two main contributions to the thesis;

1. The design of an access control framework called ACOF that protects personal health records on mobile phones. Contrary to other approaches, the framework supports secure sharing of personal records even when the hospital servers are offline.
2. The design and implementation of the PHR system that provides self-protecting Personal Health Records (PHRs) on the mobile phone. The system enables end-users to securely download and update their medical records using an Identity-Based Encryption (IBE) architecture.

6.1 Revisiting ACOF Requirements

ACOF, as the name suggests, is an access control framework that protects patients' health records beyond the hospital's trust boundaries. To achieve this, the framework considers the following issues;

User-Centric Health Record Management: One of the most important requirements of ACOF architecture is to empower patients securely own their medical records. As discussed in chapter three, previously published research relating to the protection of PHRs by individual users has been limited in developed countries due to developed infrastructure.

Offline Access Control of EHRs: Traditionally, access control in EHR systems is accomplished by storing health information in a centralised location such as the hospital server. However, when the server fails or become unavailable, for example due to frequent power outages and/or unstable Internet connections that is common in developing countries, access control decisions cannot be made, making EHR systems unusable. The daily power outages and unreliable Internet connections mandate that patients be given offline access to support their healthcare.

There are number of approaches that support offline access of electronic health records (Li et al., 2013; Dmitrienko et al., 2013; Akinyele et al., 2011). Among these approaches is the use of mobile phones to provide instant access of personal information when the hospital servers are offline (Akinyele et al., 2011). However, for end-users, such as healthcare professionals and patients to successfully utilise PHR services through mobile phones, security must be guaranteed (Zheng, 2011; Wang et al., 2012).

6.2 Design Considerations

Similar to desktop-based PHR systems, mobile phone-based PHRs must provide the following functions to the user: confidentiality and integrity of data, user authentication, and none repudiation (Avancha et al., 2012; Dmitrienko et al., 2013). Technologies that apply these security elements to mobile phones must be able to provide end-users with the same level of security as with desktop computers (Schwingenschlögl et al., 2006).

Many security protocols on desktop PCs and most security applications for PHRs are based on public key cryptography (Zheng, 2011; Hsieh & Chen, 2012; Hupperich et al., 2012; Li et al., 2013). The Public Key Infrastructure (PKI) applies a public key cryptographic method to transmit a user's public key in a secure and reliable channel (Housley, Polk, Ford, & Solo, 2002; Lee, Lee, & Song, 2007). However, it is difficult to apply PKI protocols for security in mobile phones (Sax et al., 2005; Lee et al., 2007). First, mobile phones have major limitations of performance such as less memory and less powerful Central Processing Unit (CPU). Similarly, because mobile phones form part of the wireless environment, they present a constrained communication due to less bandwidth (Lee et al., 2007). For a PKI protocol to work successfully, a mobile phone must generate a public key pair and compute a digital signature using the key. A public key certificate is then issued to the mobile through a wireless Internet connection. The public key certificate provides a method to bind the public key and its owner (Lee et al., 2007). Using the certificate, the mobile entity must authenticate itself and make secure channel for Internet service such as a PHR service. These operations are somewhat expensive when running on a mobile phone (Akinyele et al., 2011).

In this chapter, we introduce an IBE inspired architecture that supports secure sharing of personal health records on a mobile phone. To achieve this, the architecture enables end-users to securely download and update their medical records onto the mobile phone, and selectively share them with the healthcare providers in an offline mode i.e. when hospital servers are offline due to unstable main electricity and/or unreliable Internet connection. This reduces the need to rely on online access control authorities in the provision of PHRs. Figure 6.1 presents the overall structure of ACOF.

6.3 Revisiting Identity-Based Encryption Architecture

As described in chapter three, Identity-Based Encryption (IBE) offers more flexibility than Public Key Cryptography (PKC). It forms the foundation for a secure environment that separates authentication from encryption. The separation of authentication from encryption is important because it enables organizations to utilize existing mechanisms to authenticate users. Finally, IBE is inexpensive to operate and supports off-line capability. Users of IBE system do not need to check any online resource for decryption keys. Specifically, an IBE scheme has been partitioned into four sections;

1. **Setup:** Generates global system parameters and a master-key,
2. **Extract:** Uses the master-key to generate the private key, corresponding to an arbitrary public key string ID (Say mobile phone number, email address etc.)
3. **Encrypt:** Encrypts messages using the public key ID,
4. **Decrypt:** Decrypts messages using the corresponding private key

6.4 Framework Overview

Figure 6.1 presents the overall structure of the ACOF architecture. It is a four-module architecture that provides secure sharing of personal health information beyond the hospital's trust boundaries. The modules (registration module, authentication module, prescription module, and encryption module) interact with each other to support self-protection of PHRs and offline access.

The registration module comprises a registration service that enables end-users such as healthcare providers to create an account for patients. Any user who wants to receive a copy of their personal records on a mobile phone has to register to the registration service (RS). The RS is a web interface that captures users' information such as identification number, date of birth, email address, and also provides the option to select the security level. The registered Identification Number is the corresponding ID for each user. At this point, for the submission of users' information, the use of SSL is inevitable (Benaloh et al., 2009). Similarly, as demonstrated in the previous studies, a password-based solution is also used to protect the private key as it is being sent to the corresponding entity (Garson & Adams, 2008).

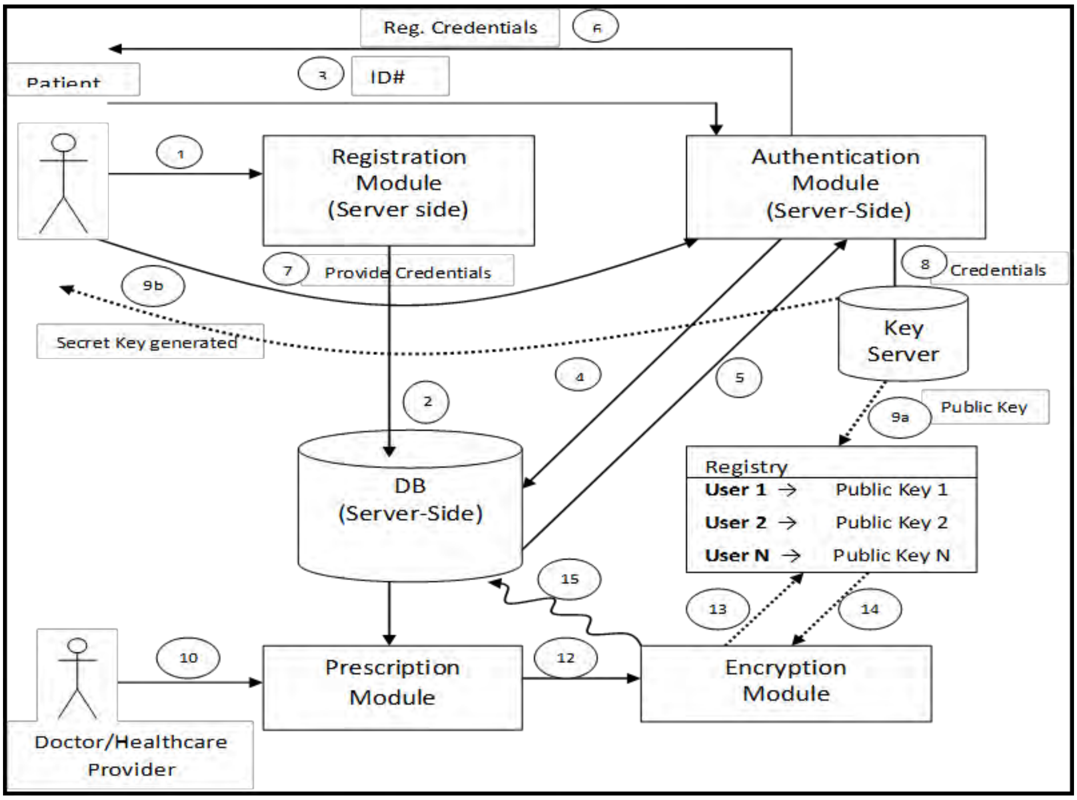


Figure 6.1: The ACOF Architecture

After signing up to the server, the registration service updates the list of the registered users with the new user's credentials. Any user listed to the RS can download and view the encrypted records stored at the hospital server.

The authentication module is responsible for authenticating users to the key server called the Trust Authority (TA) in order to calculate users' private keys. Any registered user can send a private key request to the TA in order to receive the private key. For security reasons, the transmitted key is encrypted using an IBE scheme. Besides, TA issues private keys after requesting the list of users' IDs and the corresponding selection of system parameters.

The authentication module was designed on the assumption that the trust authority service is running on a secure and protected hospital server, accessible only by the authorised hospital administrators. This is achieved by configuring the hospital server with the anti-virus software and a local firewall, which prevent illegitimate traffic traveling from the Internet to the hospital server (Joshi, Aref, Ghafoor, & Spafford, 2001; Garson & Adams, 2008).

When a new or modified record is submitted for storage to the hospital sever, the prescription module parses the records to the encryption module where sensitive parts are selected for encryption using a 128-bit AES session key. Figure 6.2 shows the high-level architecture of our framework.

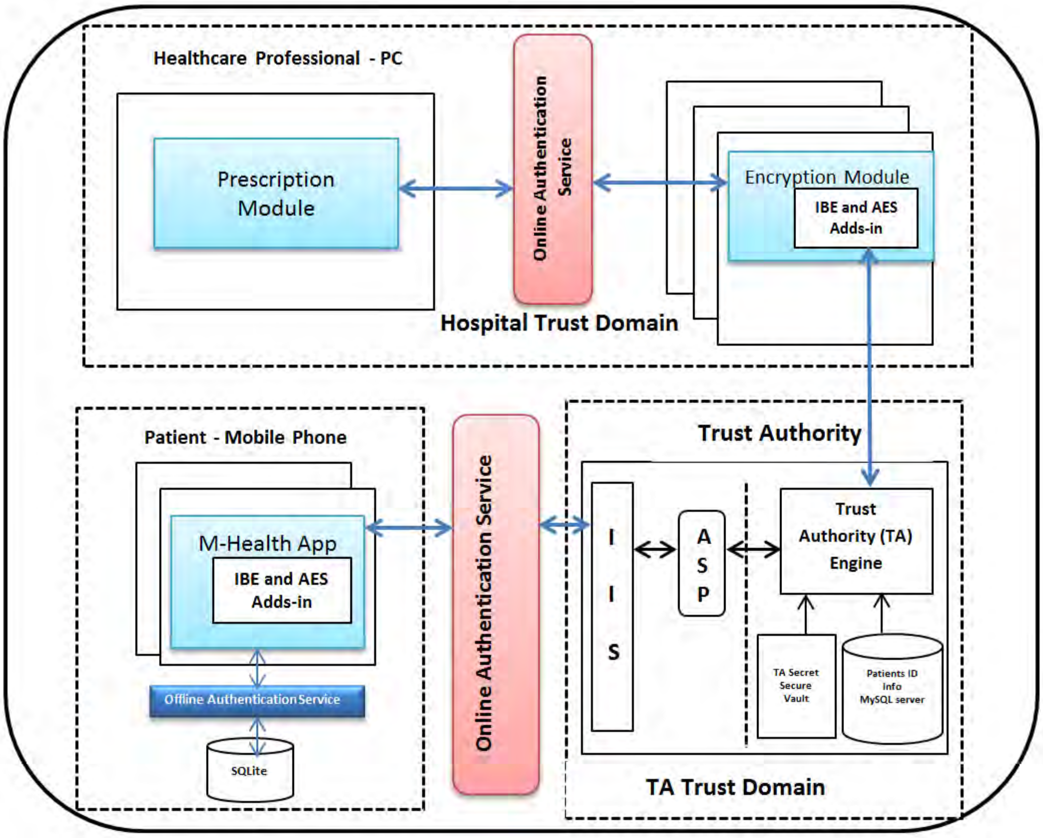


Figure 6.2: High level system architecture

For efficiency purposes, our architecture use a standard hybrid approach where records are encrypted using a 128 bit AES session key and the session key is protected using an IBE scheme. The protected session key is then transferred to patient's mobile phone. Once records have been encrypted, the encrypted records can then be stored at the hospital own server and/or exported to the patient's mobile phone along with metadata, which includes the encrypted symmetric key and the associated disclosure policies. The hash value derived from these policies is encrypted along with the session key for an integrity check. The architecture is a form of public key encryption and the corresponding private keys are generated by the key server. The key server or the Trusted Authority (TA) uses the patient's credentials (originally submitted to the RS) to generate the private key. For security reasons, private key is then used to protect the session key before it is delivered onto the patient's mobile phone.

The Trust Authority (TA) includes the following sub-components;

1. **A back-end trust authority engine**
   The trust authority engine is responsible for making authorisation decisions basing on IBE library to generate the decryption keys.
2. **A trust authority secret and secure vault.**
   This is responsible for storing the trust authority secrets. Only secure https connections are accepted from the users. Hospital administrators are responsible to run the server and the trusted authority service.
3. **A Secured MySQL Server Database.**
   In association with the trust authority, a protected MySQL database contains an up-to-date association of users' identities that enable TA to generate private keys. Trust hospital administrators run and update the hospital database.

All other IBE cryptographic operations (except the private key generation), are performed by the end-user mobile application (M-Health App). Users can download the M-Health App from the hospital web page, and after configuring it, they can view and share their records selectively. Additionally, users obtain the private key through the M-Health App without any need for an external import or copy-paste of the private key. The only action required is to send a private key request to the TA and the private key is then transfer and stored to the appropriate location on mobile phone. The M-Health App incorporates the elliptic curves (discussed later) to secure communications over the Internet and other forms of communications. Figure 6.3 shows the interactions of RS, TA and the user (M-Health App).

6.5 Offline Mobile Access

To enable mobile access, the M-Health App system incorporates the "push model" where the hospital server takes the initiative to "push" the modified records to the intended patient, either on a regular basis via schedule or asynchronously by sending an update notification. Once the updated and encrypted records are downloaded to the mobile phone, the M-Health App then breaks down the records into an XML hierarchical structure such that records can be viewed/shared selectively. However, only users with a PIN that satisfies the policy are able to decrypt. Users are authenticated via a PIN in order to retrieve and download the encrypted records from the hospital server to the mobile phone. The M-Health App then uses IBE private key stored in the Android keystore to decrypt the records in order to support offline access.

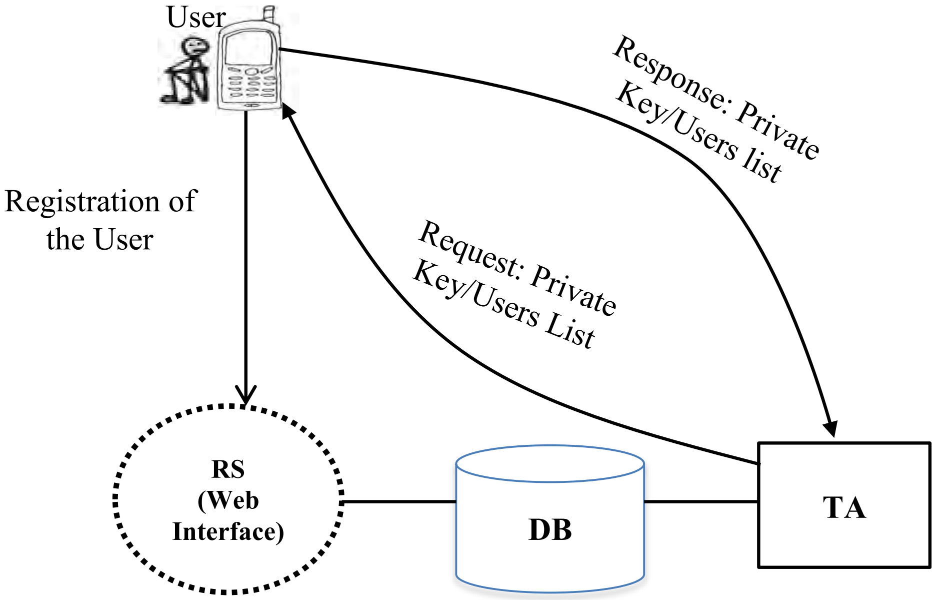

User
Response: Private Key/Users list
Registration of the User
Request: Private Key/Users List
RS (Web Interface)
DB
TA

Figure 6.3: The Interaction of RS, TA and M-Health App

6.6 ‘‘Pushing’’ Personal Health Information to the End-user

The M-Health App system incorporates a ‘‘push’’ content service that enables end-users to update their records with minimal intervention. This service involves automatic user notification and dynamic updating of personal health information to the mobile phone.

To illustrate, let us assume that a patient is interested to keep a particular section (e.g. Allergies) of his record up to-date. While browsing M-Health App system, it is likely that no content exists for this section of his record. The patient then registers to the “push content” service. Upon the completion of the registration, the server forks a dedicated thread called a monitoring agent (MA) that periodically checks the database for new content. On the event of having new information added by the healthcare giver, the MA creates XML code with the description of the added record(s), stores the XML file in the database and notifies the patient through an

SMS message. The patient is then given the option to update his records with the new modified records.

6.7 Securing Records on the Mobile Phone

The M-Health App system supports caching of encrypted records on the mobile phone to support instant sharing of health records when network connectivity is not available. However, this poses some security risks. As noted by Benaloh et al. (2009), end-users want to view plaintext of their records, but also protect it from adversaries who can mount offline attacks on the device. Therefore, the M-Health App system relies on the temporary storage to display the plaintext records. An advantage of the *tmp* directory is that the system deletes all the data stored in the directory when the user exits the application (Azadegan, Yu, Liu, Sistani, & Acharya, 2012). The encrypted XML-based records are written in the system's local filesystem and remains protected due to the IBE encryption system.

6.8 Example Scenario

Consider the case of a hospital where a clinical officer interacts with a patient. When the clinical officer submits a new or modified record for storage at the hospital server, the record is parsed into the prescription module where sensitive parts are selected for encryption by the encryption module. The encrypted records are then transferred to the hospital's own server for storage and can also be exported to the patient's mobile phone to facilitate offline access. Users (Patients and healthcare workers) whose IDs satisfy the access policy are able to decrypt the records.

In order to access the data, a patient presents his/her credentials to the hospital. Since some developing countries do not have national IDs, potential alternatives for identification may include: passport, driving permit, and National Social Security Card (NSSC). Once the patient has been authenticated, the hospital key server generates a private key for the patient and proceeds to transfer it securely to the patient's mobile phone. Using the M-Health App system, the patient can then download his/her encrypted records as shown in Figure 6.4.

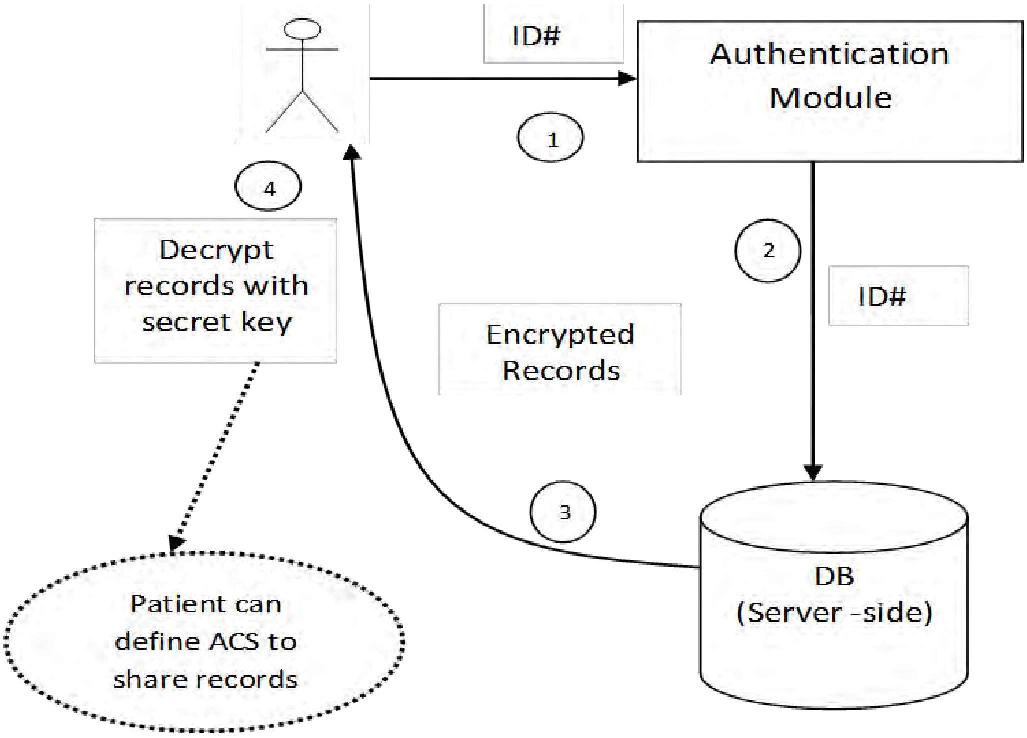

ID#
Authentication Module
1
4
2
ID#
Decrypt records with secret key
Encrypted Records
3
DB (Server -side)
Patient can define ACS to share records

Figure 6.4: Illustration of a Patient Downloading the Records

The hospital server supports only read access to the encrypted individual health records, and the encrypted records can be exported to the patient's mobile phone for portability. In order to enable offline access, the patient uses his private key (protected by IBE scheme on the mobile phone) to decrypt the records, and selectively share his records with the healthcare provider. In the next section, we describe how the patients' records are protected on mobile phone using IBE scheme and Personal Identification Number (PIN).

6.9 Security Model of the Framework

The security model of our framework combines the theoretically proven Password-Based Key Derivation Function 2 (PBKDF2) that is based on the one that Kaliski (2000) proposed, and Identity-Based Encryption scheme proposed by Shamir (1984). The PBKDF2 is a key derivation algorithm that was shown to be secure, and is part of the Rivest, Shamir and Adleman (RSA) laboratories and Public-Key Cryptography Standards (PKCS) series (Kaliski, 2000). The PBKDF2 scheme was designed to provide users communicating over an unreliable channel with a secure session key even when the password or PIN is drawn from a small set of values (Abdalla & Pointcheval, 2005). The scheme applies a one way hash function to the input along with a cryptographic salt value to produce a derived key, which is used as the AES session key in our architecture.

Similarly, as described in section 6.3 and 3.15, the Identity-Based Encryption (IBE) model is a formal security model that has been shown/proven to be secure by a number of researchers (Boneh & Franklin, 2001; Cocks, 2001). Combining the PBKDF2 and the IBE schemes integrates the security mechanisms and hence guarantees data protection. The key generation mechanism works as follows. First, the PBKDF2 scheme is used to generate a key that is derived from the user's PIN. We call this key a "Derived key" $(\mathcal{DK})$ and note that $\mathcal{DK}$ is structured as an Advanced Encryption Standard (AES) key. As a result, the $\mathcal{DK}$ is used as an AES session key to encrypt patients' records.

In the next step, we generate an AES session key (sk) using a pseudo-random number and the key $(\mathcal{DK})$. The session key (sk) is used to encrypt the patient's healthcare data on the hospital server. Finally, in order to enable the user access his/her data (e.g. to update the mobile phone version), the session key is shared with the user. We store this key securely on the mobile device/phone by protecting sk using IBE encryption on the mobile phone.

In the next section, we present the security model of our framework in detail. It involves four step namely, key generation, key encryption, data encryption, and data decryption.

6.9.1 Step 1: Key generation

The first step involves running two algorithms. The first algorithm takes as input the parameters; "SHA-1", "PIN", "Salt", "c", and "dkLen", and returns the generated derived key $(\mathcal{DK})$ for the patient's PIN. We explain what these parameters imply in the following;

- SHA-1: This is a one way hash function expressed as F: $\{0, 1\}^* \rightarrow \{0, 1\}^*$ … …………………………………………………………….. (a)
- PIN: This is the patient's PIN from which a derived key is generated. The PIN is a series of four digits that a patient randomly selects.
- Salt: This is the cryptographic salt……………………………… (b).
  The literature recommends a salt length of at least 128 bits (Turan, Barker, Burr, & Chen, 2010)
- c: This is the number of iterations……………………………. (c)
  In our architecture, we used 2000 iterations based on the previous study (Vala, Sarga, & Benda, 2013)
- dkLen: This is the length of the derived key.

The second algorithm is run by the PKG once for creating the whole IBE environment. The algorithm initialises the key server (PKG), and outputs the user's IBE key (pk). In the next subsection, we describe the applications of (a-c) above.

(a) This is a one-way hash function that is easy to compute on every input but hard to compute in the reverse direction. One-way hash functions and cryptographic hash functions in particular fall in the class of mathematical functions that are useful for personal identification, authentication and other data security applications. SHA-1 is an implementation of a cryptographic hash function designed by the United States National Security Agency, and published by the United States NIST (NIST, 2012).

(b) The Cryptographic salt is useful in creating a secure $\mathcal{DK}$. Basically, a salt is random data that is provided as additional information to the one-way hash function (SHA-1). A new salt is generated for each PIN.

(c) c is the number of iterations required within the SHA-1 function to rotate and/or shift the PIN and salt to form a derived key of length dkLEN.

The algorithms for the key generations can be expressed in pseudo-code as follows;

Algorithm 1: Key Generation

```
Input: PIN, C, dklen
Output: $\mathcal{DK}$

Begin
        Generate a 64-bit random number
        /* Pad the PIN*/
        $\mathcal{DK} \leftarrow$ SHA-1 (PIN, Salt)

/* Hash the output repeatedly for c iterations */
For (c = 0; c < 2000; c++)
  $\mathcal{DK} \leftarrow$ Hash (SHA-1, $\mathcal{DK}$, salt)
Endfor

If ($\mathcal{DK}$ > dklen)
/* Shrink $\mathcal{DK}$ */
# of blocks to delete = (length ($\mathcal{DK}$) – dklen) / block_size

   else
   /* increase $\mathcal{DK}$ to dklen */
  /* create extra blocks to fill in key length*/
  #of blocks added = $\frac{dklen - length\ (\mathcal{DK})}{block\ size}$

Endif
Output ($\mathcal{DK}$)
End
```

Algorithm 2: Session Key Generation

```
Input: $\mathcal{DK}$, Pseudo-random number (PRN)
Output: $sk$
Begin
          Generate pseudo-random number based on PIN, and personal ID details

          /* Combine $\mathcal{DK}$ and pseudo-random number to create key */

          $sk \leftarrow$ Hash (SHA-1, $\mathcal{DK}, PRS$)

Output ($sk$)
End
```

6.9.2 Step 2: Key and Data Encryption

In order to store the derived key ($\mathcal{DK}$) securely on the mobile device, the user will on receiving the key from the PKG, encrypt $\mathcal{DK}$ using his/her PIN as follows;

$$\boldsymbol{\mathcal{DK}} \xrightarrow[\boldsymbol{encrypt}]{} \boldsymbol{E_{PIN}}\ (\boldsymbol{\mathcal{DK}})$$

The PKG on the other hand will also encrypt the patient's data with the session key $(sk\ )$ as follows;

$$\boldsymbol{Data} \xrightarrow[\boldsymbol{encrypt}]{} \boldsymbol{E_{sk}}\ (\boldsymbol{Data})$$

One copy of the data is placed on the server while another is transferred to the patient's mobile device.

6.9.3 Step 3: Key Decryption Process

In order to access the data on the mobile device, a patient must first access his/her derived key $(\boldsymbol{\mathcal{DK}})$**.** This is done by requiring the patient to use his/her PIN to decrypt the encrypted key as follows;

$$\boldsymbol{E_{PIN}}\ (\boldsymbol{\mathcal{DK}}) \xrightarrow[\boldsymbol{PIN}]{} (\boldsymbol{\mathcal{DK}})$$

6.9.4 Step 4: Data Decryption

The data is then accessed by using algorithm 2 to obtain the session key (sk) that is then used to decrypt the data as follows;

$$\boldsymbol{E_{sk}\ (Data) \underset{sk}{\rightarrow} Data}$$

In order to protect the emergency records stored on the mobile phone, the architecture generates an emergency encryption key (Ek) from the user ID (ID^{*}) and encrypts the emergency records using the procedures described in sections 6.9.1, 6.9.2 and 6.9.3. The emergency data is then decrypted as follows;

$$\boldsymbol{E_{Ek}\ \left(Data_{Emergency}\right) \underset{Ek}{\rightarrow} \left(Data_{Emergency}\right)}$$

As demonstrated by Denning et al. 2010, the healthcare giver or the emergency specialist can use the patient's emergency PIN, engraved either on a medical bracelet, tattooed as a 2D bar code, or inside the cover of the mobile phone to gain access to the emergency records.

The security model of our framework rests on the security of the RSA scheme, which is a public/private key scheme based on the presumed difficulty of factoring large integers (Rivest, Shamir, & Adleman, 1978). Additionally, for efficiency reasons, we do not use the IBE scheme to directly encrypt the record data. Instead, we use an AES key wherein each data object is encrypted using an AES session key that is derived from the user's PIN using PBKDF2 algorithm, and the session key is protected using the IBE mechanism as described by Boneh and Franklin, and Cocks (Boneh & Franklin, 2001; Cocks, 2001).

6.10 Requirements for Mobile Devices-Enabled PHR Applications

The literature reveals that the design of successful mobile devices' applications involves factors related to the technical characteristics of the devices and the use of the applications (Dunlop & Brewster, 2002). These factors charge the application designers with new challenges, such as: design for mobility; design for a wide audience with various levels of competency in the use of the new technologies, that do not necessarily have a history of experience with similar applications; design for limited input/output facilities (small screen size, limited colour and font size support); and design for user multitasking (W3C, 2006; Brewster & Dunlop, 2004).

In terms of the interface design and usage, mobile phones' applications should pursue criteria similar to web sites development (Ciavarella & Paternò, 2003). The design of an appealingly pleasing interface is important, however, the success of the system is based on accessing information in an intuitive and easy way (Preece, Rogers, & Sharp, 2002).

The Canadian Heritage Information Network (CHIN) adds some practical guidelines for the graphic design of the mobile device interface (CHIN, 2004), which stretch that: each screen node of the application should fit the size of the mobile device screen; the navigation should be structured hierarchically; and backtrack and easy access to the home page should be supported. All these requirements are considered in the design of the mobile phone-based PHR system described in the next section.

6.11 System Implementation: Functionality, Features and Flow

This section picks up from chapter five – conceptual and participatory designs. In this section, we present the implementation of M-Health App system based on patients' requirements and needs described in chapter five. For example, the need to improve system navigations, terminologies, and inclusion of dates showing when a particular medication was taken. Additionally, based on the requirements identified in chapter four, it was evident that a healthcare tool that offers the following capabilities is needed;

1. Provide an offline access of patients records,
2. Empower patients to own their health records on mobile phones, given the steady increase in the ownership of the devices in Uganda.
3. Reduces the time taken by healthcare providers searching for patients' records,
4. Enable the patients to use familiar authentication methods such as PINs to minimise unauthorised access of their records.

Additionally, it was further observed that representational identifiers such as pictures and/or images are useful to semi-literate or illiterate user to navigate the PHR system (Ghosh et al., 2003; Medhi et al., 2006; Parikh & Lazowska, 2006). Therefore, we developed a PHR system distributed on mobile phone with the following features: "Login in", "Download Records", "View Records", and "Emergency Information".

Development of the system was carried out using the Android platform and J2ME. We selected Android for mobile devices due to several factors: Android was chosen because it is open source (Nauman et al., 2010); and secondly, it is the most popular operating system that runs on the widest selection of smartphones whose costs are rapidly declining (Goldman, 2011).

Similarly, Java 2 Micro Edition (J2ME) provides a platform for developing applications that are executed on resource constrained devices such as mobile phones (Lawton, 2002). Besides, it supports several security components of the standard public-key cryptosystem and other cryptographic functions (Kawahara et al., 2006). Other reasons why Java 2 Micro Edition is suitable for developing mobile phone applications include;

1. It offers strong wireless support and enables programming applications that accesses a broad range of content formats, e.g. text, XML, serialized Java objects, etc. (Kawahara et al., 2006).
2. It has the capacity to develop powerful applications, and it is platform independent. (i.e. It supports execution of application on any device supporting CLDC/MIDP, regardless of the underlying operating system)
3. Application developers can implement interactive applications with rich graphics that offer enhanced user experience, since graphics can typically be generated locally without bandwidth demand (Kenteris et al., 2009).
4. It enables synchronization between the server and mobile application (Kenteris et al., 2009).

6.11.1 Implementing IBE Architecture in M-Health App System

As stated earlier, the IBE functions only constitute part of the proposed architecture. Our aim was to develop a user-friendly PHR system that protects and securely shares patient's records on mobile phones using IBE infrastructure. To achieve this goal, there was a need for an IBE library that supports Elliptic Curve Cryptographic (ECC) operations and bilinear pairing functions (Miller, 1986; Blake, Seroussi, & Smart, 1999).

6.11.2 Bilinear Pairing

In cryptography, bilinear pairing relies on the existence of efficiently computable paring on some groups, mostly based on elliptic curves (Boneh & Franklin' 2001). It was proposed by Boneh and Franklin in 2001. The key advantage of bilinear paring is that key generation is efficient and more precise (Joye & Neven, 2009).

6.11.3 Bilinear Pairing-Based Cryptographic Libraries

There are number of pairing-based cryptographic libraries that have been design to provide bilinear pairing functions and Elliptic Curve operations. Among the libraries include: bouncy castle library, Pairing-Based Cryptography (PBC) Library, MIRACL library, jPBC and jpair libraries. In the next subsection, we analyse some of these libraries and choose the most appropriate library for our system.

6.11.3.1 Bouncy Castle Library

Bouncy Castle is a Java implementation of cryptographic algorithms that was developed by the Legion of the Bouncy Castle (Bouncy Castle website, 2012). The Bouncy Castle package is organised so that it contains a lightweight API suitable for use in any environment including J2ME. It further contains a lightweight cryptography API for C# and provides routines for ECC functions. However, literature reveals that some of the ECC features are poorly integrated and thus not appropriate for our system (Kihidis, Chalkias, & Stephanides, 2010)

6.11.3.2 Pairing-Based Cryptography (PBC) Library

The Pairing-Based Cryptography provides a lightweight cryptography API for the C language (Stanford website, 2012). It provides routines such as elliptic curve generation, elliptic curve arithmetic and Weil pairing implementation. The drawback of PBC library in regard to our architecture is the use of C programming language for the development of IBE functions. Once used in our architecture, it involves the “porting” of the code from C to Java and this will add unnecessary complexity to our system and thus do not offer a feasible solution for our case.

6.11.3.3 Performance Measurements

Dong (2010) performed an experiment on MacBook Pro (2.5 GHZ Core Duo, 4G Ram comparing the performance of IBE libraries; jpair (Dong, 2010); MIRACL (MIRACL crypto SDK website, 2012); jPBC (jPBC website, 2012), and PBC (Stanford website, 2012). Table 6.1 below describes the results.

Table 6-1: Performance Analysis of IBE libraries

Nos.	Library	Performance (Msec)	Environment	Analysis
1	MIRACL	13	C/C++	Shareware, dependencies on external libraries
2	jPBC	16	Java port	Dependencies on external libraries
3	PBC	2	C	Dependencies on external libraries
4	jpair	13	Purely Java	No dependencies, and Android supported library

Results from Table 6.1 indicate that jpair and MIRACL are the fastest IBE libraries taking 13 msec, followed by jPBC with 16 msec. This means that jpair and MIRACL are appropriate for our system. However, since MIRACL is a C software library, porting C to Java will create several overheads (Kihidis et al., 2010). Therefore, jpair remains the most suitable IBE library for our architecture. It is a Java implementation with no dependencies on external libraries. More specifically, jpair supports the supersingular curve $y^2 = x^3 + x$ over the field F_p for some prime p = 3 mod 4. An advantage of using this curve is that the number of points on the curve is exactly p+1 and so, you can generate the parameters of a random pairing easily (Dong, 2010).

6.11.4 Implementing jpair Library in M-Health App System

As stated earlier, the IBE library implemented in our system is jpair. An advantage of using jpair library is that it was implemented using Java, and has no dependencies on external libraries. Table 6.2 in Appendix 6.1 presents the symbolic representation of jpair operations used in our system. These operations are combined with AES operations (Figure 6.5) in order to support secure and efficient processing of patients' records. The operations are classified into five steps (described in section 6.10): Key generation, data encryption, key encryption, key decryption and data decryption.

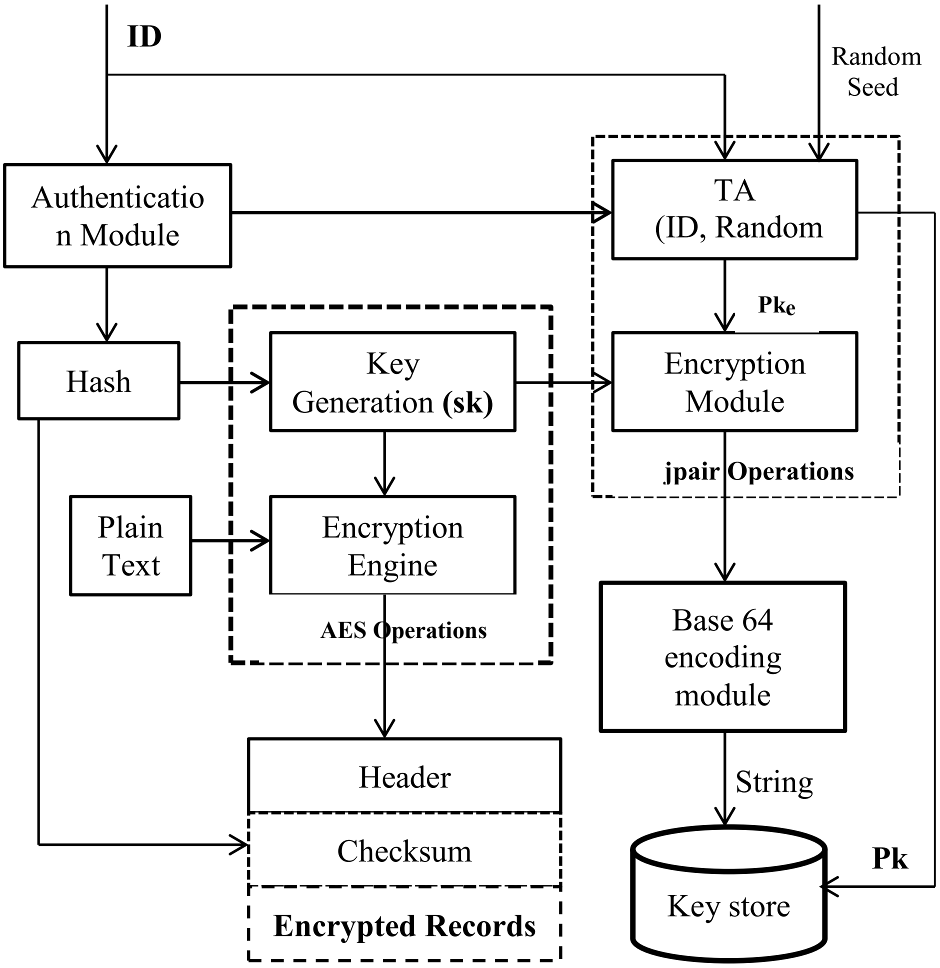


Figure 6.5: The Inner Processes of the Encryption Operations of our Architecture sk represents the session key, Pk$_e$ and Pk$_d$ represents the public and private keys computed by the TA)

6.12 Programming M-Health App System

We prototype our system based on the jpair operations described in section 6.11.3.3. Our aim was to provide a user-friendly PHR system that enables patient-users import their health records from the server and view health reports on a mobile phone. To achieve this goal, we implemented the system with two major functions: “download the records” and “view records”. Figure 6.7 shows the interaction of the components of M-Health App interfaces.

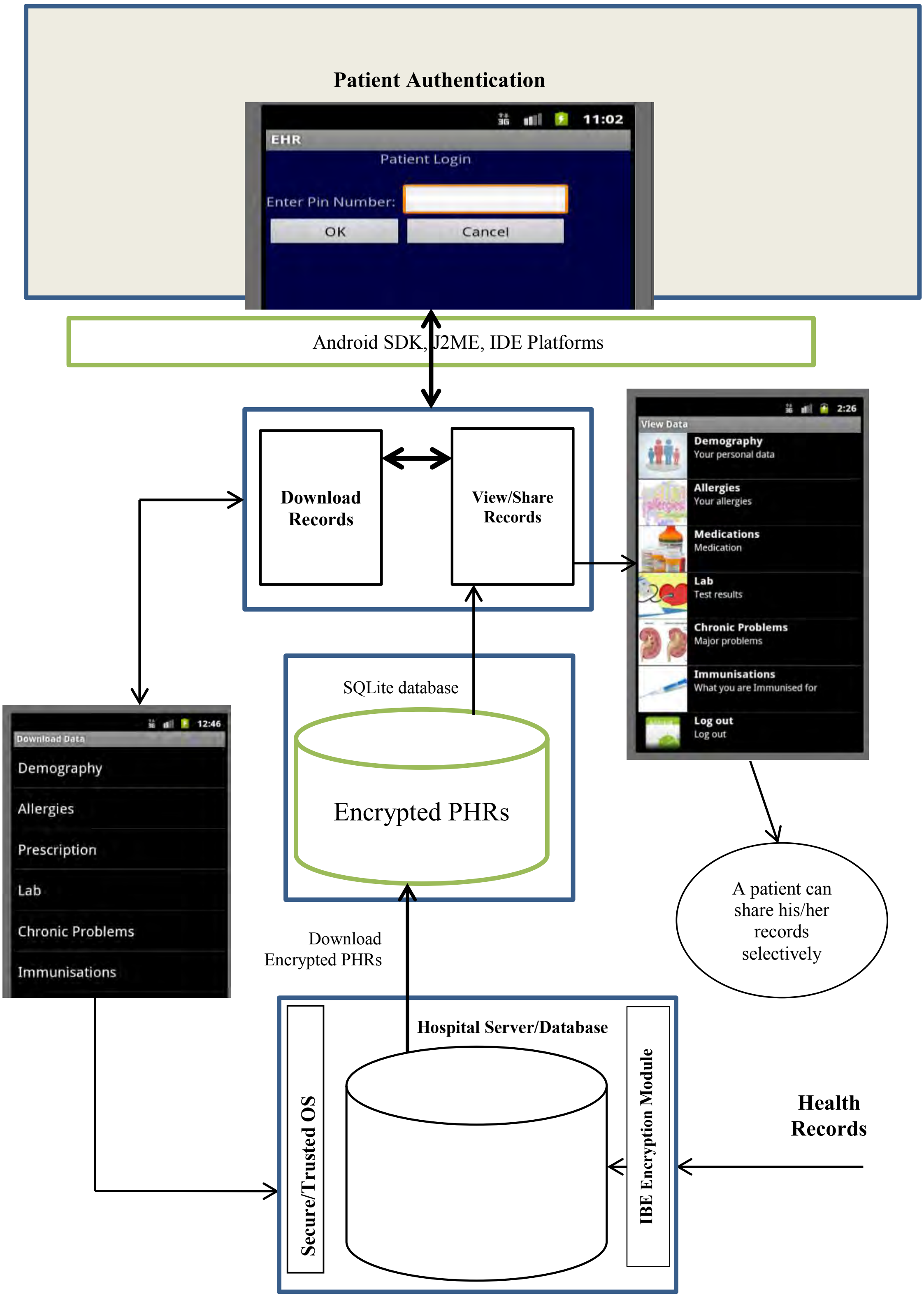


Figure 6.7: The interactions of the components of the M-Health App interfaces

6.12.1 Downloading the Records

Figure 6.7 shows the components of M-Health App system. When a user selects “download records”, the PHR system will ask the patient-user to enter a PIN and download the requested records. If the PIN corresponds to the user’s identity, the PHR system will download the records to the mobile phone. Otherwise, it will alert the users that they do not have proper access rights. Downloading personal health records from the hospital server is performed once in order to support mobility. Figure 6.6 shows the implementation of this process.

```
1.  db = openOrCreateDatabase("EHR.db", SQLiteDatabase.CREATE_IF_NECESSARY, null);
2.  // When a list is Selected
3.  Protected void onlistitemClick(listView 1, View v, int position, long id) {

4.  if(item.equals("Demography")){
5.  try{
6.  creatNewDB();
7.  // Get demography data from the server database
8.  String str_dataobj=cmn.downloadData("serializerdemo.php?PatientID="+PatientID);

9.  if(!dbinst.checkIftableExist(db,"tbl_demographykey"))
10. {
11. // Create the table for the first time
12. dbinst.createTable("tbl_demographykey",db);
13. // Create a key table for the first time
14. dbinst.createKeyTable("tbl_key",db);
15. }
16. //get the data from the server
17. String strdata=dbinst.getData(str_dataobj); // return the data
18. String struserID=dbinst.getUserID(str_dataobj);//return user ID
19. String strkey=dbinst.getUserKey(str_dataobj);// return the jpair key
20. String strkeyjavax=dbinst.getUserKeyJavax(str_dataobj);// return the session key

21. // insert the data into SQLite database
22. dbinst.insertTable("tbl_demographykey", db, struserID,strdata,strkey);
23. // save the encrypted session key
24. dbinst.insertKeyTable("tbl_key", db, struserID,strkeyjavax);
25. }
26. db.close();
```

Figure 6.6: Downloading Records from the Server to the Mobile Phone

Figure 6.6 above shows the implementation of “Download Records” function. When a list is selected e.g. demography, the M-Health App system automatically creates a database called EHR.db with Android SQLite database where the encrypted records are stored (line 6). If the database exists, it skips this stage and continues downloading the records. Jpair classes and objects are serialised (Dong, 2010) and hence the need to serialise M-Health App classes. (line 8). The M-Health App then creates a table called tbl_demography (line 12) with EHR.db, gets the demographic data from the hospital server and saves the data in EHR.db. All the processes are done without end-user's knowledge.

6.12.2 Viewing the Records

Viewing individual records is the most complex activity in our application. It involves four tasks, all combined together in order to decrypt and view the records. It involves;

1. Locating the records in the SQLite database (EHR.db) with the corresponding decryption key,
2. Decrypt the session key with IBE private key,
3. Organise the records into hierarchical data structure such that records are viewed selectively,
4. Use the session key to decrypt the records.

6.12.3 Implementation – Viewing the Records

Figure 6.8 shows the implementation of "View Records" function. When the list is selected (e.g. demography or emergency information) the M-Health App request the keys from the keystore that corresponds with patient's PIN (lines 5 and 7), converts the jpair key string to a BFCtext object (line 9) in order to decrypt the session key (line 11). The session key is then used to decrypt the records e.g. emergency information, and finally the Application displays the records. When the user exist the application, the system automatically deletes all the data in the temporary storage of the application. To protect patient's records from adversaries who can mount offline attack on the phone, the records cached on mobile phone remains protected using identity-based encryption architecture.

As discussed in section 6.2, the key challenge in developing a successful mobile phone-based PHR application is the constraints imposed by the devices such as processor constraints, memory restrictions and battery life. To cater for these constraints, the M-Health App system performs "lazy" decryption i.e. only decrypting records on an as-needed basis. This means that less memory and processing power is used and thus conserving battery life.

Similarly, to improve usability of our system, the user only has to select the decryption option once. As the user views other encrypted sections, the entries are automatically decrypted in the background in order to utilise the phone memory efficiently (Android developer reference, 2013).

```
if(j==0) // where j is an integer holding the position of our structure – (Demography, Allergies, Prescription, Lab, etc.)
{
try{
// get the jpairkey from the key store
PrivateKey keyjpair=cmn.getKeyObject(info.getKey());
//Query the key store and get the session key
String javaxkeyfromdb=dbinst.queryKey(db,cmn.getUserID());
//Convert the jpair keystring to a BFCtext object
BFCtext javaxkey=cmn.getDataObject(javaxkeyfromdb);
//Decrypt the session key with jpair key
String decryptedkey=cmn.decrypt(javaxkey, keyjpair);

// convert the session key to a Key object
 javakey=(java.security.Key)b64.decodeToObject(decryptedkey);
// pass data for decryption and display
//  String strText=cmn.decrypt(cmn.getDataObject(info.getData()),
 cmn.getKeyObject(info.getKey()));
System.out.println("Decrypted array data is  "+info.getData());

}
db.close
```

Figure 6.8: Viewing Records on Mobile Phone

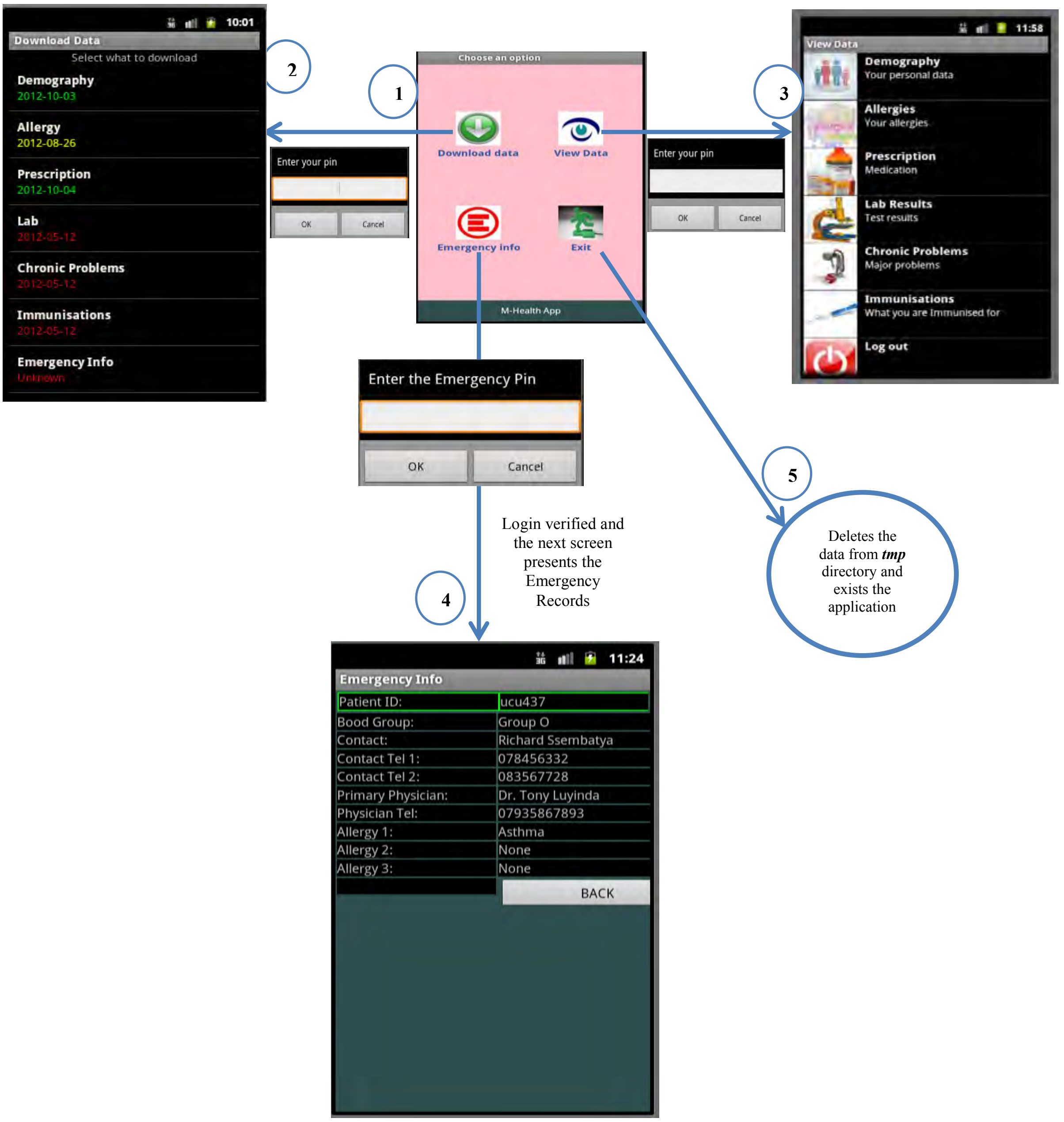
6.12.4 Functionality and Screenshots of the Interfaces of the M-Health App System

Figure 6.8 shows the screenshots of the interfaces of the M-Health App system. In the first step, the user or the hospital administrator downloads the generated APK file (saved on the hospital server) to the user's mobile device. Upon completion of the APK file download to the mobile device, the application is installed and loaded by the local AMS module[15] (integrated within the Android platform). When the user starts the application, the AMS retrieves a file containing the Java code for the M-health App graphical user interface and displays the application menu shown in Figure 6.9. The application contains a user-friendly menu that allows easy browsing of the PHR Content.

For the end-user to download his/her records, he/she enters his/her ID through the phone keyboard, and the application notifies the user that a secure connection has been established. Once a PHR block (e.g. demography) is "touched", the application uses the established connection and downloads the record from the hospital server to the mobile phone. The same

[15] Application management software (AMS) controls the management (start, termination) of M-Health App execution as well as their installation. The AMS is typically provided by the device's manufacturer.

procedure applies when viewing the records. However, view the records function is executed in a standalone mode with no wireless connectivity requirement. The user later synchronizes to the backend server only to update the originally selected PHR content.



Select what to download

Demography
2012-10-03

Allergy
2012-08-26

Prescription
2012-10-04

Lab
2012-05-12

Chronic Problems
2012-05-12

Immunisations
2012-05-12

Emergency Info
Unknown

Login verified and the next screen presents the Emergency Records

Deletes the data from ***tmp*** directory and exists the application

Emergency Info

Patient ID:	ucu437
Bood Group:	Group O
Contact:	Richard Ssembatya
Contact Tel 1:	078456332
Contact Tel 2:	083567728
Primary Physician:	Dr. Tony Luyinda
Physician Tel:	07935867893
Allergy 1:	Asthma
Allergy 2:	None
Allergy 3:	None

Figure 6.9: Screenshots of the interfaces of the working M-Health App system. Interface (1) is the first interface when the user launch the application, interface (2) enables users to download/update their records from the server – (green colour = records are up to date, yellow colour = never downloaded the records and Red colour = Records are outdated). Interface (3) enables users to selectively view and/or share their records. Exist and Log out functions enables the system to delete all data stored in the tmp directory when the user exits the application.

6.13 Summary

In this chapter, we have described the development and implementation of PHR system distributed across mobile phones with a security model and an interface that supports the usage and concerns of low literacy users in developing countries. Additionally, the chapter demonstrates four key advantages of ACOF architecture for rural healthcare;

1. **Offline Mobile Access:** ACOF mobile application enables patients to securely download and update their medical records onto the mobile phone, and securely share their health records with the healthcare providers in an offline mode i.e. when the hospital servers are offline due to unstable main electricity and/or unreliable Internet connections.
2. **End-to-end encryption:** Contrary to the previous approaches, our architecture is designed to secure patient's records right from the entry point at the hospital, all the way to the recipient (mobile phones). This maintains confidentiality of records towards users and support portability.
3. **Content-based Access Control.** Our system provides content-based access control, where access control decisions are applied at the level of the individual record node (e.g. lab results) within the patient's health record. An advantage of this approach is that individuals are explicitly authorised to access only specific portion of the record. For example, a pharmacist dispensing medications may need access to an individual's current prescription information, but does not need read access to the patient's allergies and lab results. The selective sharing of personal information is defined via hierarchical data structure, where a patient's record is decomposed into a set of categories such as medication, allergies, immunisation etc.
4. **Patient-Centric**. In ACOF, patients are having full control of their medical records and can effectively share their health records with a wide range of healthcare professionals. To deal with the potential risks of privacy exposure especially in mobile phone-based PHR environment, ACOF takes the same patient-controlled approach as advocated by Benaloh et al. (2009) and Li et al. (2010). The patient (who is the PHR owner) has full control over the selective sharing of their data using access control and encryption schemes. In addition, each PHR owner generates his own decryption key to prevent thefts or compromises by the unauthorised parties.

"Usability testing should never be used to determine what users need.
It is for catching bugs"
- Don Norman

CHAPTER SEVEN: M-Health App System Evaluations and Results

7. Introduction

This chapter describes the evaluation methods performed on the M-Health App system in two different settings: controlled setting and field study. The chapter describes the methods used in these experiments, the parameters studied and the final evaluation results. The aim of this evaluation was to answer research questions three and four of this study, that is to say, to test whether the ACOF architecture can be usable on a mobile phone without interfering with the 'normal' use of the device in terms of its efficiency, performance and resources management; and identify the usefulness of the PHR system distributed on mobile phone to end-users including patients and healthcare providers. Two prototypes of the M-Health App system were evaluated. The first prototype of M-Health App was evaluated for performance evaluation and usability. The feedback obtained through these evaluations was then used to improve the system to produce a second prototype. The second prototype was then implemented and the field study evaluation carried out.

The M-Health App system performance evaluation was conducted through laboratory experiments, and usability evaluation was carried out through standard usability evaluation procedures. The procedures and results of the performance and usability evaluations are reported in sections 7.3.1 and 7.3.5 respectively.

From the performance and usability evaluations, conclusions were drawn about the usability of mobile phone-based PHR system in relation to the research questions. The conclusions drawn are then presented in the next chapter – chapter eight.

7.1 M-Health App System Evaluation

According to Nielsen (1993), evaluation is an attempt to assess the value of an innovation or technology to end users. In the simplest term, Scriven (1991) described evaluation as the systematic determination of the quality or value of the system. Thus, evaluation is an integral part of the design process, which focusses on usability of the system and user's experience when interacting with the system (Rogers et al., 2011). Gould and Lewis (1985) reason that reviewing or demonstrating a system to end-users without studying how easily users can learn and use the system, may result in a misleading conclusion. What is required first is usability testing, where end-users are given simple tasks to carry out, and their performance, thoughts and attitude analysed (Gould & Lewis, 1985).

The most used definition of usability is from International Organisation for standardisation (ISO9241). Usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO usability guidelines, 1998). Thus, the focus of usability by ISO9241 was primarily the degree at which a system is effective, efficient and satisfying.

Nielsen, one of the foremost and internationally recognised usability experts proposed an expanded definition of usability, and includes the following five attributes (Nielsen, 1993);

Efficiency: The system should be efficient to use, so that once the users have learned the system, a high level of productivity is possible.

Learnability: The system should be easy to learn so that users can quickly get work done by the system.

Errors: The system should have a low error rate, so that users make few errors during the use of the system. Additionally, if users make errors, then they should easily recover from them. In the context of this research, an error is any action that does not accomplish the desired goal, and the counting of such actions provides a measure of a system's error rate (Nielsen, 1993).

Memorability: They system should be easy to remember such that casual users are able to return to the system after some period of time of not using it.

Satisfaction: The system should be pleasant to users, so that end-users are subjectively satisfied when using it, and they like it.

In addition to Nielsen's (1993) attributes, Preece et al. (1994) added throughput, flexibility and user attitude towards the system. However, throughput is comparable to Nielsen's efficiency; flexibility refers to the extent to which the system can accommodate tasks or environments and attitude is comparable to Nielsen's user satisfaction (Haklay & Tobón, 2003).

All these aspects relate to intrinsic objectives of our study: exploring the utility of PHR systems in the developing countries, where the majority of end-users come from disadvantaged background such as lower literacy among others. In this case, the principles of usability evaluation methods provide a sound base for the appraisal of PHR systems in developing countries.

7.2 Usability Testing

Madrigal and McClain (2010) gave practical guidance that includes a list of dos and don'ts of usability testing. In their research findings, they pointed out that usability testing is among the least glamorous, but most important aspect of user experience research. On the other hand, Lewis and Rieman (1994) described that usability evaluation techniques such as narratives and explanations of study participants through the think-aloud method, or post-study open-ended interviews should be used for the systems' evaluation in order to ascertain differences in problem-solving abilities between users, differences in difficulty between tasks and the effects of instruction (Van Someren, Barnard, & Sandberg, 1994).

Rogers et al. (2011) classified usability testing/evaluation into three broad categories, depending on the setting, user involvement, and level of control. The classified evaluations include: controlled settings that involves end-users such as laboratories or living labs, where users' activities are controlled in order to measure or observe certain behaviours; natural settings such as field studies, where users are evaluated in their natural settings, primarily to facilitate the introduction of the new technology; and any settings that don't involve users, where researchers imagine or model the system that is assumed usable to end-users.

In this study, the M-Health App system was tested and evaluated using all three categories. First, the evaluation that don't require the users was done at the university laboratory in order to establish whether the M-Health App architecture can be usable on mobile phone without interfering with the 'normal' use of the device in terms of its efficiency, performance and resources management. Secondly, Heuristic Evaluation was conducted in order to identify errors, comprehensibility and any other HCI related concerns that may discourage or stop end-users from using the system (Nielsen, 1994a; Mack & Nielsen, 1994; Jones and Marsden, 2006). Thirdly, user experience evaluation was conducted to find out whether the system's instructions are adequately clear and also to identify bugs that may be overlooked during the Heuristic Evaluation (Vermeeren et al., 2010). Finally, after the laboratory evaluation, the M-Health App system was tested in the field (field study) to determine the usefulness of mobile phone-based PHR system to the users including healthcare professionals and the patients. At every stage of the evaluation, there was a need to loop back to the earlier stages, which made development to occur in iterative cycles of assessing-designing-testing-analyzing-refining-testing-analyzing-refining (Nielsen, 1993).

7.3 Laboratory and Performance Evaluation of M-Health App System

Four laboratory evaluation sessions that included computational performance evaluation, Heuristic Evaluation, user experience evaluation and focus group evaluation were conducted in a controlled, laboratory setting to obtain feedback from users on the acceptability and functionality of the M-Health App system. For the first evaluation sessions, several experiments were conducted. First, we measured the efficiency (download time) required to download the records from the server to the mobile phone using four different 3G cellular networks in Uganda, as well as decryption performance on the mobile phone. To show that our architecture induce acceptable costs in terms of records storage, we also measured the cipher-text size overhead incurred by our encryption architecture. Our aim was to establish whether the M-Health App system can be usable on mobile phone.

7.3.1 M-Health App System Performance Evaluation

In order to better evaluate the performance of our crypto-based PHR system distributed on mobile devices, we measured the efficiency of IBE decryption on a mobile phone. We used a Huawei *IDEOS* phone, running Android OS, with 256MB of RAM and GT-I9100 Samsung, running Android OS with 1GB of RAM. Our motive was to show the abilities of different platforms. We conducted this experiment using a small set of medical records that contained a representation of the PHRs from the Allan Galpin Health Centre. The records included demographic information, allergies, prescription, lab results, chronic problems and immunisation. Figure 7.1 summarises the measurements conducted on the two mobile devices. The x-axis represents the structure of PHRS (bytes) and y-axis shows the time required for decryption.

The results from Figure 7.1 demonstrate that the average decryption time of Huawei IDEOS mobile phone is 7.5 seconds while the average decryption time for GT-I9100 is 1.4 seconds. The difference in decryption time is attributed to many factors including processor and memory capabilities (Dmitrienko et al., 2013). Comparing the decryption time of PHRs on the two devices and the recommended waiting time (Nielsen, 1997; Zona, 1999), we assert that the decryption time of PHRs on the two platforms have acceptable performance.

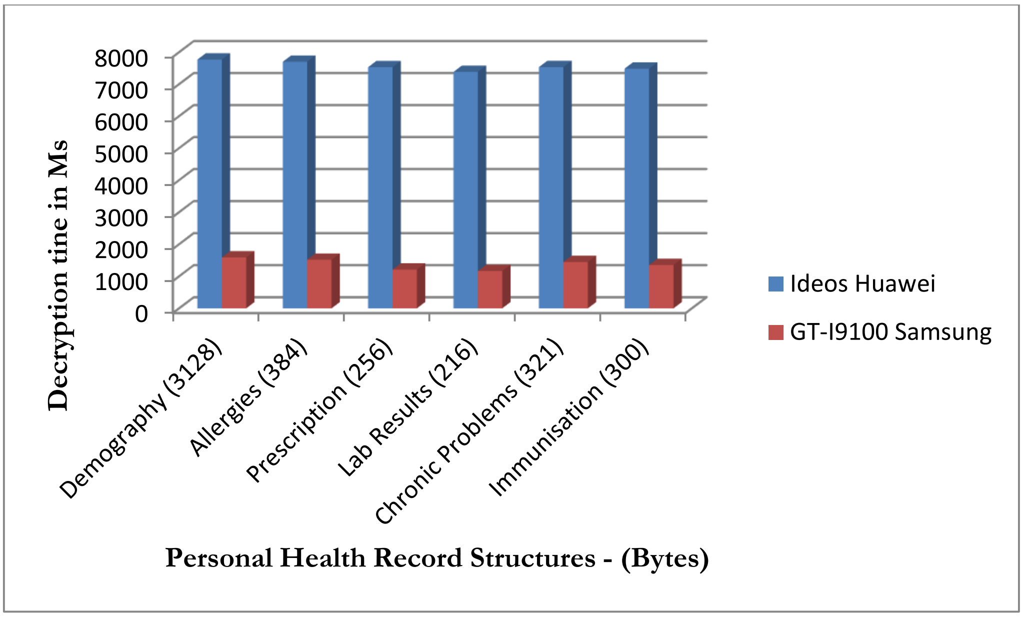


Figure 7.1: Decryption time (Huawei *IDEOS* and GT-I9100 Samsung)

Furthermore, our results indicate that although the encrypted records vary in size; i.e. demograhy (3128 bytes) allergies (384 bytes), prescription (256 bytes), lab results (216 bytes), chronic problems (321 bytes) and immunisatoin (300 bytes), there appear to be no direct relationship/corroletion between the record's size and time taken to decypt the records. This is attributed to the fact that the M-Health App system provides a standard procedure to perform the decryption: locate the IBE key from the keystore, decrypt the session key with IBE private key, and then use the session key to decrypt the records. Likewise, the system employs a standard hybrid approach where records are encrypted using a 128 bit AES session key and the session key is protected using an IBE encryption scheme, which was asserted by Akinyele et al. (2011) in order to improve the efficiency of the mobile phone-based EHR system.

7.3.2 M-Health App System Storage Overhead Evaluation

Akinyele et al. (2011) described the procedures of measuring the storage overhead of the mobile phone-based encryption architecture. In the same study, they determined the storage overhead incurred by their solution, by conducting an experiment on a set of medical records obtained from Vanderbilt University Medical Center (VUMC). The records were stripped of personally identifying information that contained a representative of clinical documents. The total size of the record set was 8.3MB. After encrypting the record set, the storage overhead incurred by their solution increased from 8.3MB to 46MB, which is 554.2% increase.

To determine the storage overhead incurred by our architecture, we extend the methods used by Akinyele et al. (2011) and conducted an experiment from a set of health records obtained from the Allan Galpin Health Centre. The records contained a representative of medical documents that includes demographic information, allergies, prescriptions, laboratory results, chronic problems and immunisation. The size (in bytes) of each portion of the records described include: demography (2070), allergies (261), prescriptions (167), laboratory results (143), chronic problems (211) and immunisation (202). To measure the storage overhead, we wrote a Java application that calculates the actual content/record size. Figure 7.2 describes our results. We note that the storage overhead of our architecture increased from 3054B to 4605B (150.8% increase), which is smaller compared to that of Akinyele et al. (2011). Therefore, we believe that the storage overhead incurred by our architecture is still in an acceptable range.

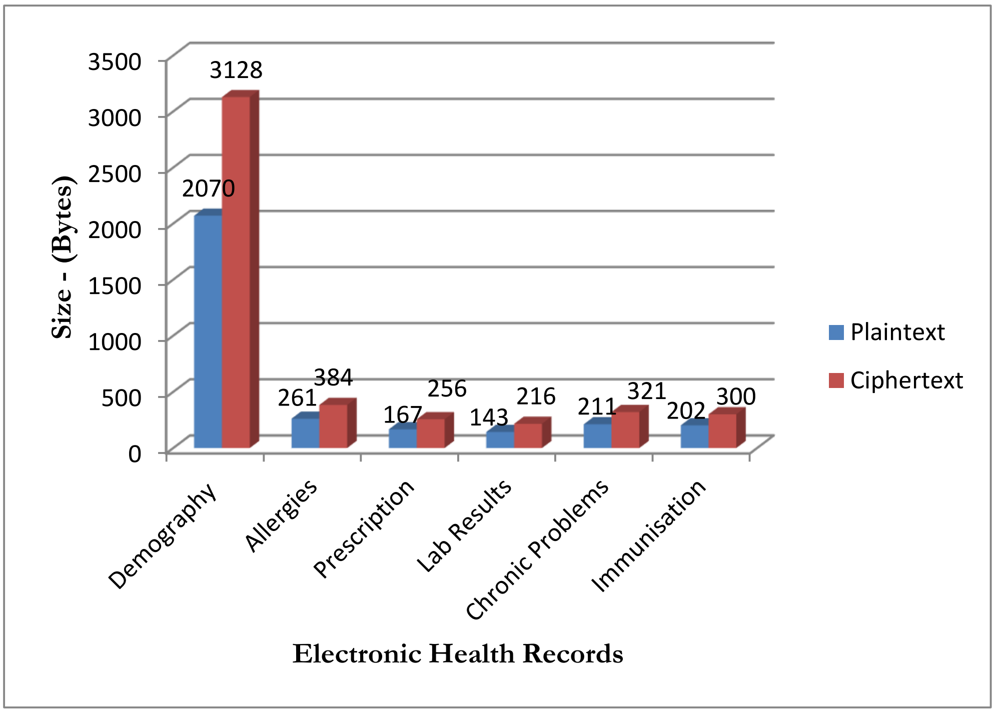


Figure 7.2: Storage overhead incurred by our architecture

7.3.3 Download Performance and Waiting Time Evaluation

According to Nielsen (1999), download performance/speed is the "single-most important design criterion on the Web". End-users are constantly demanding faster content downloads (Nielsen, 2000). Although long download time of Internet content has been a consistent problem encountered by the majority of Internet users (Selvidge, 2003; Lightner, Bose, & Salvendy, 1996; Pitkow & Kehoe, 1996), it is still controversial as to what constitutes an acceptable download time for a typical Internet-based download (Bailey, 2001). For example, Nielsen (1997) advocates for 10s limit, while Zona (1999) recommends 8s. Additionally, Bouch, Kuchinsky and Bhatti (2000) conducted a study attempting to identify how long users would wait for pages to load. In their study, users were presented with Web pages that had predetermined delays ranging from 2 to 73 seconds. While performing the tasks, users rated the latency[16] (delay) for each page they accessed as good (Up to 5 seconds), average (6 – 10 seconds) and poor (over 10 seconds). The conflicting evidence in the literature was also highlighted and examined by Hoxmeier and DiCesare (2000), who observed the performance intentions at 12s.

The download time is affected by a number of factors: the performance of the browser, the speed of the Internet connection, the local network traffic, the load on the remote host, and the structure and format of the content requested (Nah, 2004). In this study, we are not addressing the issue of how these factors can be balanced to produce an acceptable download time but rather, we are interested in finding out whether our PHR system generates tolerable download time described by Nielsen, Zona and, Hoxmeier and DiCesare (Nielsen, 1997; Zona, 1999; Hoxmeier & DiCesare, 2000).

7.3.3.1 Experimental Setup

We measured the efficiency (download time) of downloading the records from the server to the mobile phone using 3G cellular networks and WLAN 802.11. Our evaluation methods were based on the study conducted by Ekler, Nurminen and Kiss (2008). In their work, they described the implementation of a BitTorrent based P2P application for low end mobile devices and analysed its performance over 3G networks and WLAN.

The experiments were done with Huawei *IDEOS* phone, running Android OS, with 256MB of RAM. The size of the encrypted records stored on MySQL database varied from 216 Bytes to 3128 Bytes. We used two different setups to connect to the web server in order to measure the efficiency of M-Health App download architecture;

[16] According to Bouch et al. (2000), latency is the delay between a request for a Web page and receiving that page.

1) The mobile phone was connected via 3G cellular networks to the Internet and the download time measured. Figures 7.3 (a-c) describe a summary of our results and appendix 7.2 shows a detailed description of the results.
2) The mobile phone was also connected via WLAN, connected via ADSL connection to the Internet. Time taken to download the records from the server to the mobile phone was recorded and saved to the server. Figure 7.4 describes our results.

7.3.3.2 Evaluation: Waiting Time with 3G Cellular Network

Figures 7.3 (a-c) presents the average waiting time of a two-week experiment in which personal health records were downloaded from different places, at the same times, using the four 3G mobile networks in Uganda (MTN, Orange, Warid and Airtel). Although Uganda has more 3G mobile networks, the four were preferred because of the low barrier for setting up Internet access services on mobile phones. Three experiments were conducted each day at the same time in four different places: Kampala city, Mukono, Buddo and Nsangi and at different intervals: 8:30-11:30am, 12:30-4:00pm and 4:30-8:30pm. The differences in intervals were due to the fact that we wanted to establish the best time interval\range for patients to download their records efficiently. Figures 7.3 (a-c) shows the average waiting time to download personal health records from the server, running an apache web server application.

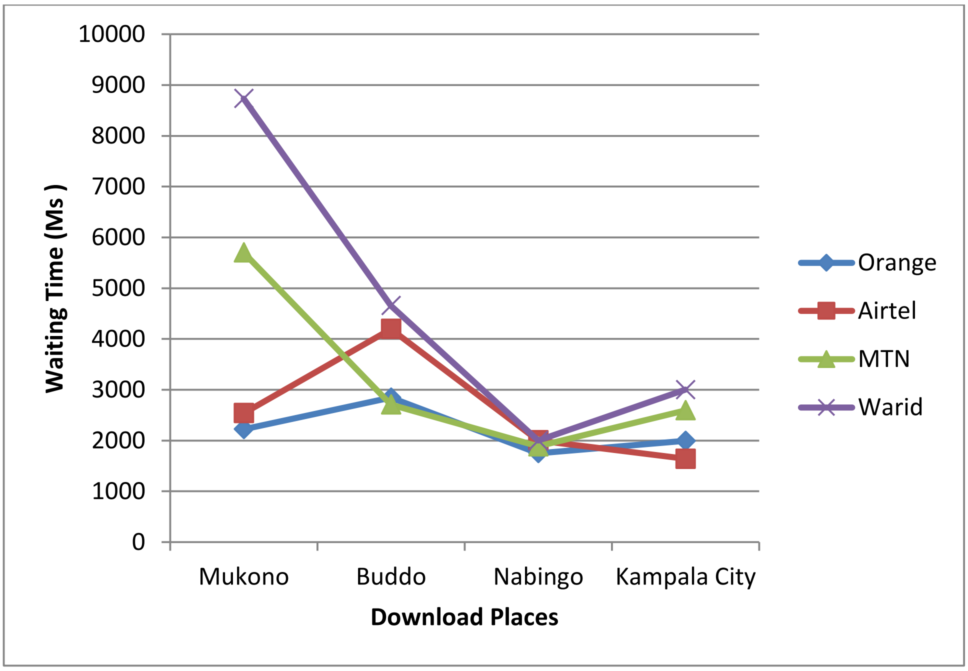


Figure 7.3 (a): Average waiting time – (8:30 – 11:30am) in four places at the same time

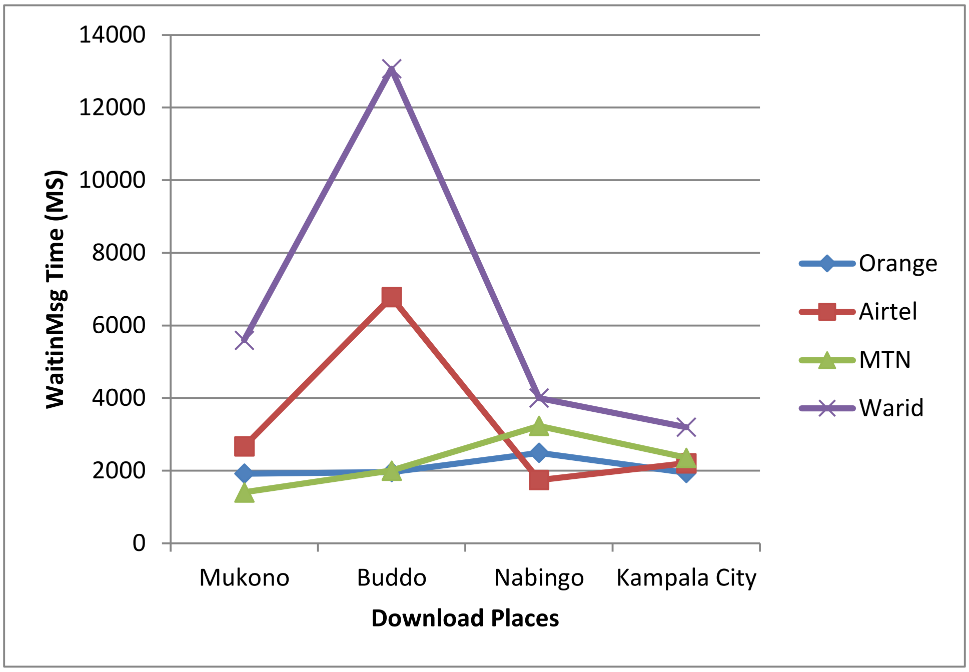


Figure 7.3 (b): Average waiting time – (12:30 – 4:00am) in four places at the same time

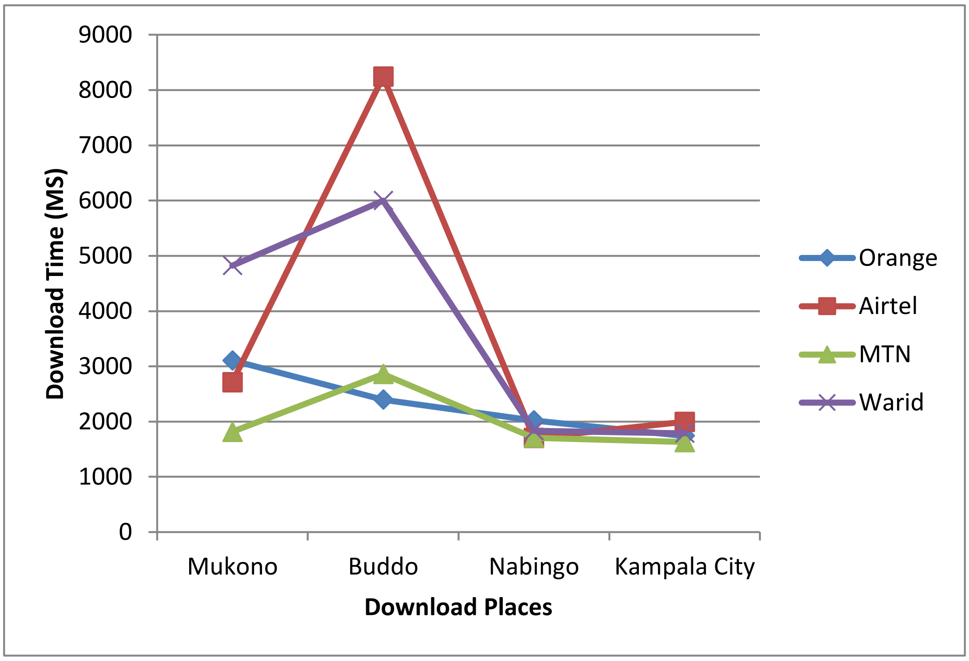


Figure 7.3 (c): Average waiting time – (4:30 – 8:30am) in four places at the same time

7.3.3.3 Analysis and Description: Waiting Time with 3G Cellular Network

Figures 7.3 (a-c) show the distribution of time taken to download the records from the server to a mobile phone using 3G cellular networks (MTN, Orange, Warid and Airtel) in Uganda. The vertical axis represents the time taken to download the records and the horizontal axis represents the structured personal health records. As shown in Figures 7.3 (a-c), the average waiting/download time of personal health records of sizes (in bytes) between 216 and 3128 on 3G cellular network is 6.5 seconds. The prolonged waiting time was observed during the peak hours (12:30-4:00pm), which greatly improved after 4pm. Comparing the M-Health App waiting time with Nielsen's recommended time, we conclude that our system offers tolerable download time using 3G cellular networks.

7.3.4 Evaluation: Waiting Time with Wireless LAN

We further conducted a one-day experiment using WLAN technology from the Uganda Christian University (UCU) network. We used UCU wireless network because the University had extended its wireless connection to the Allan Galpin Health Centre. After obtaining approval from the University authorities, we connected the experimental mobile phones via ADSL connection and the time taken to download the records was recorded by the server. Figure 7.4 below describes our results.

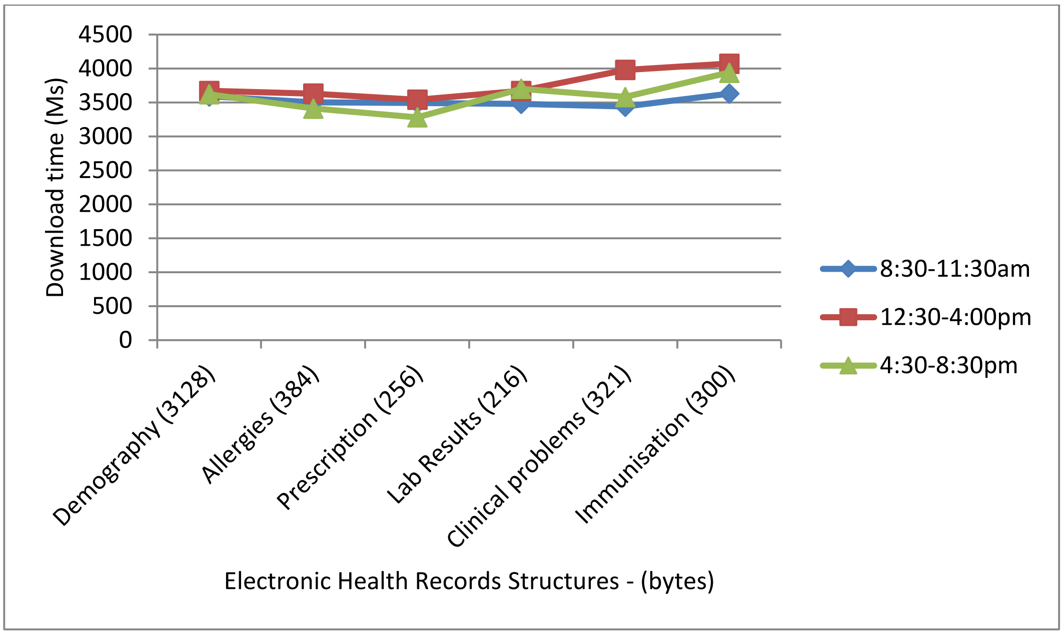


Figure 7.4: Download time – WLAN technologies

7.3.4.1 Analysis and Description: Waiting Time with Wireless LAN

The results from Figure 7.4 above indicate that the average waiting time of our system to download the records from the server is 3.5 seconds in the morning, 3.8 seconds in the afternoon, and 3.4 seconds in the evening. This shows that our system generates acceptable waiting time, as recommended by Nielsen (1997); Zona (1999); Bouch et al., (2000); and Hoxmeier & DiCesare (2000).

Additionally, contrary to the 3G cellular networks, the waiting time of M-Health App system to download the records on WLAN environment is faster than that of 3G cellular networks. Ekler et al. (2008) observed that the higher bandwidth provided by WLAN technologies creates a performance gap between the 3G mobile networks and the WLAN technologies. Results from Figure 7.4 indicates that the waiting time for 3G cellular networks is twice that of the UCU WLAN – assuming other factors remain constant. This means that the WLAN should be the preferred choice for our architecture, if available. However, the wider coverage of 3G cellular networks will allow downloads to proceed even if the patient is on the move.

7.4 M-Health App System: Usability Considerations, Evaluation and Testing

Usability is an important facet of the overall quality of interactive applications. Usability is traditionally applied to general presentation and behaviour features of a system, such as interface design, choice of the icons, interaction style, and abstraction from the specific nature of the application (Mayhew, 1991; Nielsen, 1993; Shackel, 1991; Garzotto, Matera, & Paolini, 1998; Ghosh et al., 2003; Medhi et al., 2006).

There are a number of studies that have proposed usability factors and how each may be measured during usability testing sessions (Reed, 1992; Guillemette, 1995; Zhang and Adipat 2005). These factors were measured empirically and repeatedly throughout the evaluation process. In the next section, we present the usability reflections taken into consideration and the results of the usability tests performed on M-Health App system with the assistance of the end-users.

7.5 M-Health App System Usability qualities and considerations

As described in section 6.10, the M-Health App system has been designed taking into account several usability guidelines collected from relevant studies associated to three main characteristics of mobile applications: small screens, limited input and processing, and mobility;

1. The system is designed for mobility by providing an intuitive interface with simple dialogues, short and concise information so that interaction with the application requires minimal effort (Zhang & Adipat 2005).
2. The interface is appealing to a wide range of users with various skills and expertise (Jones & Marsden, 2006).
3. The system's presentation follows a hierarchical multi-level structure that helps end-users to easily browse and understand information of their interest (Buyukkokten et al., 2002; Jones & Marsden, 2006).
4. The menus are designed in order to help users easily reach the desired information (Chittaro & Dal Cin, 2002; Parikh & Lazowska, 2006). Menus are clearly and consistently labeled with icons to help users with simple navigation, learnability and memorability (Nielsen, 1990). To minimize cognitive load, long lists of choices have been avoided and backtrack and easy access to earlier pages/home page is supported (Bederson, Clamage, Czerwinski, & Robertson, 2003).
5. The content page information is fitted on one screen to avoid scrolling (Jones & Marsden, 2006).

Therefore, these requirements were considered in the testing of the mobile phone-based PHR system described in section 6.12.4.

7.6 M-Health App System Usability Evaluation and Testing

Nielsen and Molich (1990) identified four ways to evaluate a user interface: formally by analysis technique; automatically by a computerized procedure; empirically by experiments with test users; and heuristically by simply looking at the interface and passing judgement according to one's own opinion. Although analysis models are useful in analysing objects, Nielsen and Molich (1990) affirmed that they have not reached the stage where they can be generally applied to software development projects. Similarly, automatic evaluation is completely infeasible, except for a few very primitive checks. Therefore, current practices engage empirical and heuristic evaluations, if one wants a good and thorough evaluation of a user interface (Nielsen and Molich (1990).

In our study, usability tests of the M-Health App system and interfaces were performed both empirically and heuristically. During these tests, participants were asked to accomplish specific tasks (identified with users in section 5.5) using M-Health App system. These tasks were also reviewed and agreed with the clinical officer at AGHC. The tasks include;

1. **Task 1**: Select the content item (M-Health_App.APK) from the website and then download it directly to the mobile device through a mobile network and the Internet.
2. **Task 2**: Install the M-Health_App.APK directly to the personal mobile phone.
3. **Task 3**: Use the PIN given to you and download your medical records from the healthcare server.
4. **Task 4**: View and share the following types of records on your mobile device with the clinical officer
    a. Demographic Information
    b. Medications
    c. Previous Lab results
    d. Allergies
    e. Immunisation
    f. Emergency information
5. Task 5: Logout the application

7.6.1 M-Health App System Heuristic Evaluation

Heuristic Evaluation is an informal method of usability analysis where a number of experts (normally in that particular field) are presented with an interface design and asked to comment on it (Nielsen & Molich, 1990). Heuristic Evaluation is done by looking at an interface and trying to come up with an opinion about what is good and bad about the interface. Ideally, HCI experts conduct such evaluations according to certain rules such as those described by Nielsen & Molich (1990), and Nielsen (1994b).

In this evaluation, five Human Computer Interactions (HCI) specialists conducted the heuristic evaluation using the 10 usability heuristics described by Nielsen (Nielsen, 1994b), and we observed all the testing sessions. The number of evaluators was based on Nielson's argument that there is no need for more than five evaluators. Our aim was to test the application for simplicity, efficiency, errors, comprehensibility and any other HCI related concerns (Rogers et al., 2011; Jones & Marsden, 2006).

The evaluation was useful because multiple perspectives and recommendations were obtained, and several issues discussed. For example, all the five HCI specialist agreed that there is a need to include an action and progress bars in the application especially when downloading and encrypting the records.

Additionally, three of the HCI specialist noted the unprofessional way of displaying the application menu when the system is launched (Figure 7.5), and recommended that the application menu should be displayed using Android dashboard. Other HCI concerns included: date showing when the patients last downloaded their records should be colour-coded to support illiterate users; differentiate records that are out-dated from up-dated records and, getting rid of toast messages such as “on successful decryption”. Appendix 7.1 shows the description of heuristic illustrations obtained from the evaluation. This type of evaluation was useful because we obtained multiple perspectives about recommendations and solutions, which was then used to improve our system.

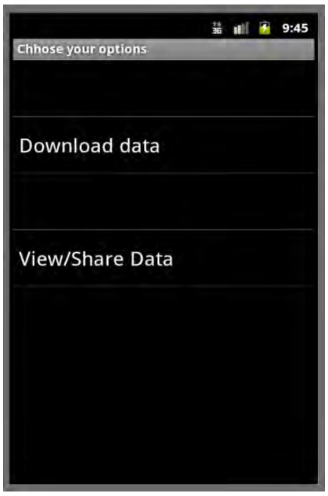


Figure 7.5: Screen element showing application menu before Heuristic Evaluation

7.6.2 M-Health App System User Experience Evaluation

According to Obrist, Roto, and Väänänen-Vainio-Mattila (2009), user experience is about how users feel about using a designed prototype. The ISO DIS 9241-210:2008 describes user experience as a person's perceptions and responses that result from the use and/or anticipated use of a system or service (ISO, 2008). Therefore, the user experience evaluation of the M-Health App system was conducted to find out end-user’s response and perception before the system is rolled out. Our aim was to determine whether the M-Health App instructions are adequately clear and also to identify bugs that may be overlooked during the expert evaluation.

The user experience evaluation was done at the Allan Galpin Health Centre between January and February 2013. Verbal announcements through the clinical officer were made inviting patients to participate in the evaluation. Six (6) patients volunteered to participate in the evaluation. Six mobile phones were provided and participants were met in groups of twos in a controlled environment. Participants were asked to accomplish a set of tasks using the application (M-Health App). Our aim was to identify any functional error/(s) and flaws that could have skipped the attention of the expert evaluators. We used observations and interviews during and after the use of the application in order to get information about user's reactions to the application (Arhippainen and Tähti, 2003). The observation focused on users' facial expressions and behaviour in general (Dabbs et al. 2009). During the test, the observations about users' gestures and behaviours were recorded and discussed during the interview. Participants were also asked to "think aloud" during the test. The whole evaluation per group including interviews took between 25 and 35 minutes.

The feedback from this evaluation was further used to improve our application. Most crucially, participants noted that, when an interrupt occurs during the use of the application, the system terminates the entirely application, prompting the user to start afresh. This prompted us to modify our prototype before the next stage of evaluation. Additionally, participants found the font too small and difficult to read in low light conditions. To address these problems, we increased the font size in the next version of our system and taught the end-users how to adjust the contrast of the display with considerations of the battery life.

7.6.3 M-Health App System Focus Group Evaluation

According to Marczak and Sewell (2006), focus groups were originally called "focused interviews" or "group depth interviews". The technique was developed after World War II to evaluate audience response to radio programs (Stewart & Shamdasani, 2007). Since then scientists and HCI evaluators have found focus groups to be useful in understanding how or why people hold certain beliefs about a system of interest (O'Donnell, Scobie, and Baxter, 1991).

A focus group is an interacting group of 6-9 users (Nielsen, 1997b), having some common interest or characteristics, brought together by the evaluator, who uses the group and its interaction as a way to gain information about the features of a user interface (Nielsen, 1997b; Preece et al., 2002), tasked completed, learnability and ease of use of the application (Kenteris et al., 2009). In the view of that, focus group evaluation of M-Health App system was conducted to evaluate the percentage of tasks completed, time needed to complete the tasks and Learnability.

For the purpose of analysing and understanding how users perform their tasks, HCI literature advocates the complete recording of the interactive session using the audio or video recorders and the computer screens (Lewis & Rieman, 1994). The recordings assist in analysing what the participants viewed on the screen during the session and provide a better understanding of the relationship between the specific images that appear at a specific point (Haklay & Tobón, 2003). Additionally, they can also be used to time different tasks and evaluate the performance of participants in accomplishing the tasks.

Building on this background, we conducted a focus group evaluation with real users who were randomly recruited at the Allan Galpin Health Centre, with the requirement of mobile phone usage experience (e.g. type, send and retrieve a text message). Seven (7) patients were recruited to take part in this phase of evaluation. Participants in the sample were 22-30 years old. Seven Huawei IDEOS mobile phones were provided and participants were met in groups of twos and threes in a controlled environment. These pairs were joined by three members of staff from Allan Galpin Health Centre.

During this evaluation, several quantitative usability attributes for each individual participant were measured. Out of the generic usability attributes identified by Nielsen (1993); Guillemette (1995) and Lindgaard (1994), we measured those that fit in the nature of our system. This gave better understanding about which usability problems should be given priority based on available time. Jeffrey (1994) highlighted that if 50% or more of participants have difficulty in completing a task, then this feature is considered problematic and require much attention. Below are the usability attributes measured during focus group evaluation.

1. **Effectiveness:** The percentage of tasks completed
2. **Efficiency:** Time needed to solve tasks in comparison to a pre-defined “task completion time goal”.
3. **Learnability:** The improvement in task performance in the second trial.

Each usability test session consisted of an introduction to the scope of the session and the system, the main testing tasks, a group discussion and lastly, an interview (Haklay & Tobón, 2003; Dabbs et al., 2009). The discussions focused on the usefulness and effectiveness of the M-Health App system as well as user satisfaction. The content of these interviews covered the strengths and weaknesses of the mobile phone-based PHR system when compared with the existing paper-based solution. End-users were also invited to contribute corrections and comments on the interface design.

During the introduction, the project and the M-Health App were introduced to the participants. Participants were also informed that the M-Health App is a mobile application that is meant to empower them securely and usefully own their medical records.

We tested each task independently. Lewis and Rieman (1994) recommended that tests that involve single service/task such as downloading records or viewing records generate reliable results than tests that combine tasks such as downloading records and then viewing records. Therefore, in each session, participants were given scenarios for a single task. The first session was driven by the following scenario.

Task 1 – Identify the M-Health_App APK: *Assume you are Mussa - a registered patient at Allan Galpin Health Clinic. Mussa's electronic health records are stored on the clinic's database server. Mussa is now required to download the M-Health_App APK from* *http://ictd1.cs.uct.ac.za* *to the mobile phone through a mobile network and the Internet. Please spend the next few minutes and perform this task.*

Scenario for task 2: – Installing the APK: *Assume you are Mussa - a registered patient at Allan Galpin Health Clinic. Mussa has downloaded the M-Health_App APK to his mobile phone and is now required to install the downloaded M-Health_App to the mobile phone. Please spend the next few minutes and perform this task.*

Scenario for task 3: – Downloading the records: *Assume you are Mussa - a registered patient at* Allan Galpin Health C*linic. Mussa's electronic health records are stored on the clinic's database server. Mussa is now required to use the M-Health App and download a copy of his personal health records from the server to his mobile phone using ucu222 as his PIN. Please spend the next few minutes using the M-Health App.*

Scenario for task 4: – Viewing the records: *Assume you are Mussa - a registered patient at Allan Galpin Health Clinic. Mussa's personal health records are stored on his mobile phone and now required to use the M-Health App to view the following sections of his personal health records using ucu222 as his PIN.*

a. Demographic Information
b. Medications

c. *Previous Lab results*
d. *Allergies*
e. *Immunisation*

Scenario for task 5: – Log out the Application: *Assume you are Mussa - a registered patient at Allan Galpin Health Clinic. Mussa's personal health records are stored on his mobile phone and now required to use the M-Health App to log out the application. Please spend the next few minutes using the M-Health App.*

The participants (Figure 7.6) were encouraged to use the think-aloud method while performing the intended tasks (Nielsen, 1994b). All sessions were conducted in a controlled setting in order to obtain feedback about how quickly participants can work and the number of errors committed for each task. The experiment was conducted with videotaping, but we abandoned this method for a number of reasons. First, it was not possible to aim the video recorder towards the screen and the user simultaneously. Secondly, movements by the participants made it difficult to focus the camera on the screen. As a result, we relied on observations and screen-capturing software called Camtasia[17] for Windows (TechSmith, free for 30 days) with video and audio capabilities loaded on the laptop and synchronised to wirelessly record how users make selections and navigate the system's features on the mobile phone.

Figure 7.6: Sample focus group evaluation session

The Camtasia software enabled us view the mobile phone screen on the laptop. The recordings were automatically time stamped to facilitate tagging issues of concern; tasks completed; and completion time. Lewis and Rieman (1994) affirmed that this approach gives a tester a

[17] http://www.techsmith.com/camtasia.html

machine-readable record of user actions that can be easier to summarise and access. Figure 7.7 (b) summarises the results of the quantitative usability attributes recorded throughout the usability tests. The tester's notes (taken during the session) and the laptop recordings were reviewed in conjunction with the participants to validate the findings and to elaborate the potential source of problems and errors. We also rated the significance and priority of each problem and summarised the results using the usability assessment reports.

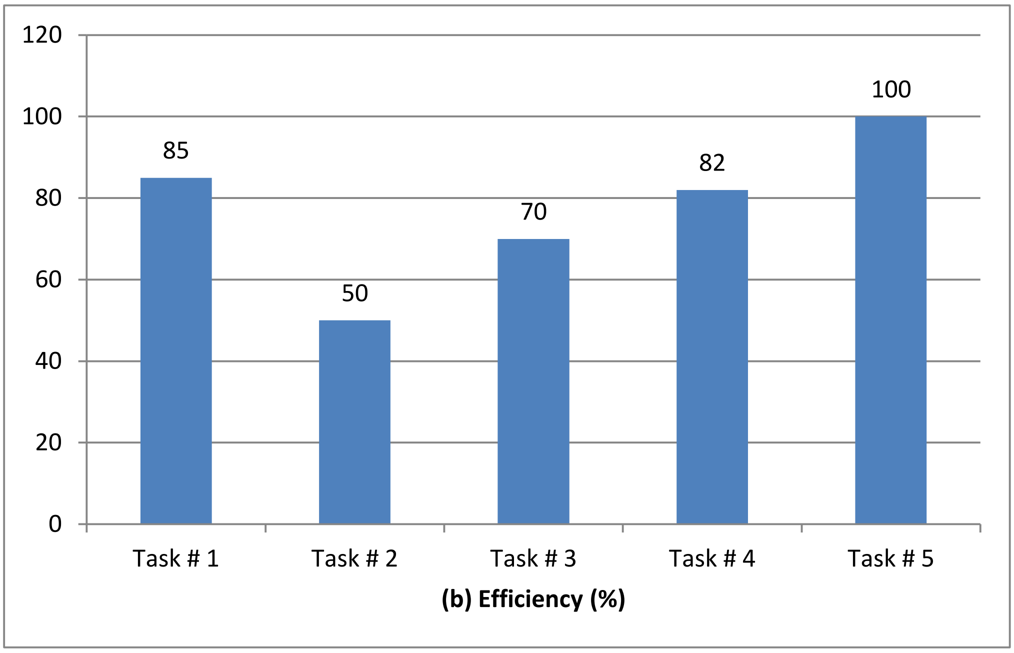


Figure 7.7 (b): Measurement of quantitative usability attributes. Efficiency: Time needed to solve tasks in comparison to a pre-defined "task completion time goal"

The learnability of M-Health App system was assessed with two measurements;

1. The improvement in task performance in the second trial (Kenteris et al., 2009), and
2. Tasks completed without errors or getting frustrated (Gitau, 2012).

These measurements were based on usage monitoring through observation, laptop recordings and oral interview (Dabbs et al., 2009). Figure 7.8 summaries the quantitative measurements obtained.

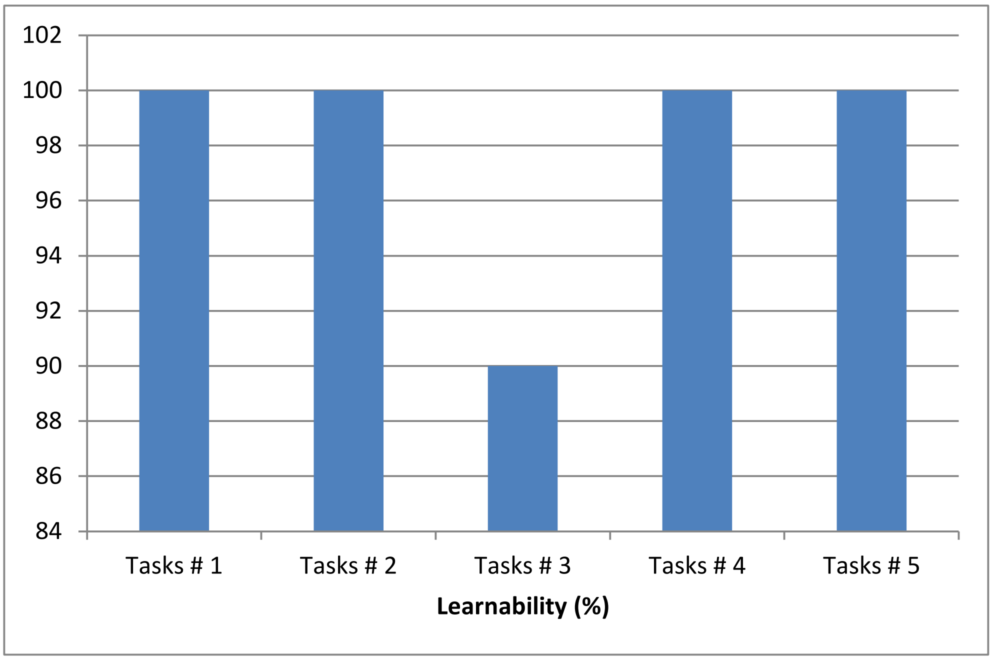


Figure 7.8: Learnability: Percentage of Tasks Completed on the second trial.

Figure 7.8 describes the parentage of tasks completed on the second trial. Interesting to note is that on average, all the tasks were completed on the second trail, and without errors or getting frustrated by the system. Only one participant experienced an error when entering the PIN due to phone keyboard. However, when tried the second time, the participant was able to complete the task.

7.6.3.1 Discussion of Focus Group Evaluation Results

As indicated in section 7.3.10, the M-Health App System focus group evaluation by patients was joined by three members of staff from the Allan Galpin Health Centre. The main reason for involving healthcare (AGHC) staff was to assess their reactions and concerns when patients are using the application. Three (3) medical practitioners voluntarily accepted to participate in this evaluation. During the evaluation, medical practitioners were briefed about the overall objective of the session, and the goals to be accomplished. Similarly, they were advised to take note of any concerns or obstacle that may hinder them from using the system. In fact, one participant volunteered to explain to patients why it is necessary to be the gatekeeper of their records.

At the end of the focus group evaluation, a focus group discussion was arranged with the medical practitioners to express their views and concerns. The discussion took place at AGHC and lasted approximately one hour. All discussions were recorded and transcripts prepared

(Haklay & Tobón, 2003). In the next section, we describe the responses and reactions observed during the focus group discussion with the medical practitioners.

7.6.3.2 Medical Practitioners' Perspective

The focus group discussion with medical practitioners demonstrated promising results towards a mobile phone-based PHR system. Before the focus group evaluation session, the medical practitioners were mixed in their opinions about providing patients access their health records on mobile phone. All predicted that the intervention would not change hard outcomes such as patients' decision making, or their relationships with their patients. Additionally, the medical practitioners wondered how health records will be updated on to a mobile phone since records are normally updated by healthcare practitioners. However, at the conclusion of the study, all the participated medical practitioners agreed that supporting patients own their medical records on mobile phones will empower them directly manage their healthcare records, and hence reduce the hospital burden of being the information gatekeeper.

"…… at the beginning, I was wondering how patients' records would be added and updated on the mobile phone. I was very confused and almost refused to participate, because I suspected that the study intends to add more work to us, which is not the case..."

"…… One of the most common obstacles to provide dependable and quality healthcare is that majority of patients don't keep their paper-based health records. In every 10 patients who visit the clinic, less than 2 provide their medical history. The system provides a better solution to the problem…."

Additionally, the medical practitioners noted that the M-Health App system provides an alternative to access patients' records when Clinic Master is offline due to power outages and unreliable Internet connections. The only challenge observed was how to encourage patients to keep their records up to-date. However, two medical practitioners reasoned that empowering patients with their records on mobile phones will give patients an incentive and it will motivate patients maintain their records.

Furthermore, although previous studies on PHR systems indicate that increasing the online update of health information by patients would decrease medical errors (Halamka et al., 2008; Hassol et al., 2004), the medical practitioner who participated in this study objected to this argument and maintain that this instead will distort the clinical encounter, since the majority of patients may not know what to add or remove. As a result, all the medical practitioners recommended that patients should be given read only access in order to minimise medical errors.

The concept of “push” personal health records to the individual owner was also observed as a key contribution to the acceptability of the M-Health App system to the medical practitioners. After realising that our system provides instant notification to patients when their records are updated, all the healthcare practitioners overwhelmingly supported the recommendation of M-Health App system to their health centre.

“… The moment you update patient’s records to the server, a patients receives a notification message to update his records. This will make our work easy, and build some confidence that patients’ information on mobile phone will be regularly up to-dated...”

The consensus opinion was that the M-Health App system will be useful from the perspective of the medical practitioners. In practice, the healthcare practitioners noted that the M-Health App system will have a positive impact in terms of increased access to health information and healthcare, improved ability to diagnose and follow-up, more timely health information and expanded access to patient’s information by healthcare professionals.

At the conclusion of this evaluation, all of the healthcare practitioners that participated in the evaluation endorsed the general concept of the M-Health App system, and all agreed that they were in support of giving patients direct access to their health records using M-Health App system.

7.6.3.3 Patients’ Views and Observations during Focus Group Evaluation

During the interviews and focus group discussions, the attitudes of patients toward M-Health App system were overwhelmingly positive. However, one major concern was observed, which affected the percentage of tasks completed (Figure 7.7 (a)). We observed that tasks # 2 (downloading the records) and tasks # 4 (viewing the records) were affected by the way users entered their PIN. We observed that users without prior knowledge of the usage of smartphone found entering the PIN challenging;

U*ser X: “…Although the application is easy to learn, the mobile device keypad is hard to use. In many attempts, it was hard for me to enter my PIN in one attempt. For example, whenever I could enter ‘r’, ‘t’ would appear…..”*

However, we noted that in the subsequent trials, users gained more experience with the mobile phone keypad, which increased the percentage of tasks completed (Figure 7.8). Interesting to note is that the decryption speed of the Huawei IDEOS phones was not an issue for the participants.

7.6.4 Aggregation of M-Health App System Laboratory Evaluation Results

At the completion of each laboratory session, we administered a reliable and valid measure of user satisfaction, the After-Scenario Questionnaire (ASQ) (Lewis, 1995), which is a three-item survey for users to rate their satisfaction with ease of completing the task, time to complete the tasks and support information using the seven-point scale (lower scores = more satisfied). Our aim was to compare the three versions of the M-Health App system after laboratory evaluations, and establish whether there was an increase in user satisfaction with the M-Health App system over time. An overall ASQ score was obtained by averaging the scores of the three versions of M-Health App system. Results from Table 7.1 indicate that, the mean ASQ scores declined from (1.89 ± 1.09) to (1 ± 0), demonstrating that there was an increase in user satisfaction with M-health App over time.

Table 7-1: Measuring whether there is an increase in user satisfaction over time. (M = mean score, SD = standard deviation)

Item	**Session 1**	**Session 2**	**Session 3**
Ease of completing tasks	M ± SD (1.78 ± 0.98)	M ± SD (1.45 ± 0.5)	M ± SD (1 ± 0)
Time to complete tasks	M ± SD (1.58 ± 0.98)	M ± SD (1.28 ± 0.25)	M ± SD (1 ± 0)
Support when completing tasks	M ± SD (2.30 ± 1.3)	M ± SD (1 ± 0)	M ± SD (1 ± 0)
Overall ASQ	**∑ (M ± SD) (1.89 ± 1.09)**	**∑ (M ± SD) (1.24 ± 0.25)**	**∑ (M ± SD) (1 ± 0)**

7.7 Field Study

There are a number of usability studies that have affirmed that field studies are the most important practices in usability evaluation (Grimes, Kantroo, & Grinter, 2010; Rogers et al., 2007; Wixon et al., 2002). Similarly, a survey conducted by Mao, Vredenburg, Smith and Carey (2005) described field studies as the most important and practical method to reveal end-user needs and satisfaction.

According to Nielsen (2002), a field study is a method for collecting data about users, and involves observation and interviewing. This enables the investigator to evaluate how users think about the system, interact and integrate the system within the settings they will ultimately be used in (Rogers et al., 2011). Additionally, Zhang and Adipat (2005) explain that usability tests of mobile phone applications through field studies reveal end-user satisfaction because it considers mobile context and unreliable wireless network connections, which are difficult to simulate in laboratory experiments. This means that the perceived benefit of the mobile application is derived based on users' experience in a real environment (Kjeldskov & Stage, 2004; Palen & Salzman, 2002).

Building on this literature, we tested the M-Health App system in the field to determine whether patients found it feasible to use independently and to assess the functionality of all of its features, including records downloading and display. Our overall aim was to explore the utility of mobile phone-based PHR system to the people leaving in developing world. Figure 6.9 describes the PHR system tested with end-users in Uganda, one of the least developed countries in the World. We chose Uganda because the principle investigator was familiar with the environment and culture of the people leaving in Uganda, and Allan Galpin Health Centre in particular.

7.7.1 Field Study Ethical Considerations

After obtaining the Institutional Review Board approval for the field study design, the selected patients signed an informed consent that included information about their willingness to use IDEOS mobile phones to access their personal health information. The institution administration gave informed consent for clinical notes to be used during the study period.

7.7.2 Recruitment of Study Patients

Patients were eligible for the study if they have used a mobile phone before, although they did not need to have access to the Internet. Patients were randomly recruited from October 2012 through November 2012 from the waiting room of the clinic. At the end of the recruitment exercise, fifteen (15) participants in total were voluntarily willing to participate in the study. 9 were males and 6 were female. The ages of the participants varied from 20 to 38 years, average being 28.5 years.

7.7.3 Data Collection and Analysis

Patients completed written questionnaires after the trial period of M-Health App system. The questionnaire (Appendix 7.4) assessed the usefulness of mobile phone-based PHR system (M-Health App system) to patients and within the context of personal health information usage. These questions were based on previous studies (Dabbs et al., 2009), and were pilot tested among different group of patients at the clinic.

7.7.4 Test tools and Procedures

In addition to user training on the use of the M-Health App system, each participant was given a simple user manual describing all the features of M-Health App system, and a mobile number to call or beep for technical help. Participants were also given an IDEOS U8150 Android phone containing 1GB memory card, charger and an Orange mobile network SIM card loaded with 75MB of data and 2500 Uganda shillings of voice to call or beep for technical help. Three of the fifteen participants tested M-Health App system on their own Android phone. Participants were also offered to use M-Health App system after the completion of the study as an incentive to participate.

The testing session consisted of an introduction to the scope of the field study, the M-Health App system and lastly, a questionnaire filled by all the participants (Dabbs et al., 2009). During the introduction, the project and the M-Health App were introduced to the participants. Some demographic information such as age, sex and education were collected as well as information about their prior knowledge regarding the use of mobile phones, touch-screen and electronic mobile health applications. Then the field study was briefly introduced to the participants. Figure 7.10 shows the characteristics of the participants. Interesting to note was that nine of the participating patients had used in the past standalone mobile applications such as calendar and games; yet, none had previous experience with electronic mobile health application usage.

7.7.5 M-Health App System Field Study Evaluation Results

Figure 7.10 presents the demographic characteristics of the enrolled participants. Because the recruitment procedure had no age restrictions, the characteristics of the enrolled participants as a whole are shown. Although we attempted to encourage patients without prior knowledge to mobile phone usage and Internet to participate in the study, nearly all of the participants had knowledge to mobile phone usage and Internet through mobile money and/or Internet banking.

Characteristics	Variables	Frequency
Sex	Female	6
	Male	9
Age (years)	20 – 38 years	
Education	University	9
	Vocational	3
	Primary School	3
Employment	Students	9
	Carpenter	2
	Messenger	4
Mobile Device use	Mobile phone	15
	Smart phones	11
	Laptop and Smart phones	10
Standalone mobile Applications use		9
Electronic mobile health Applications use		none

Figure 7.10: Characteristics of the Participants (n=15)

7.7.6 Data from M-Health App System Usage log Files

Figure 7.11 presents a histogram of the use of M-Health App system over the course of the study. On average, the M-Health App system was used daily over the three month study period. We chose a three month study based on the previous study conducted by Faridi et al. (2008). All participants used the download feature to download their records, the view records feature to view their records and only 12 participants accessed their emergency information.

The participants reported that they used download feature because it is mandatory to download the records before you view them. Of the Nine (14) subjects who viewed their records, 3 respondents described that they viewed the records to support their memory when they were buying medical drugs, 5 viewed their records to confirm accuracy, 2 viewed their records to support the nurse make decision, and 4 reviewed clinical notes to support their decision. All the 12 participants who viewed their emergency information reported that they were demonstrating the system to their friends and/or relatives.

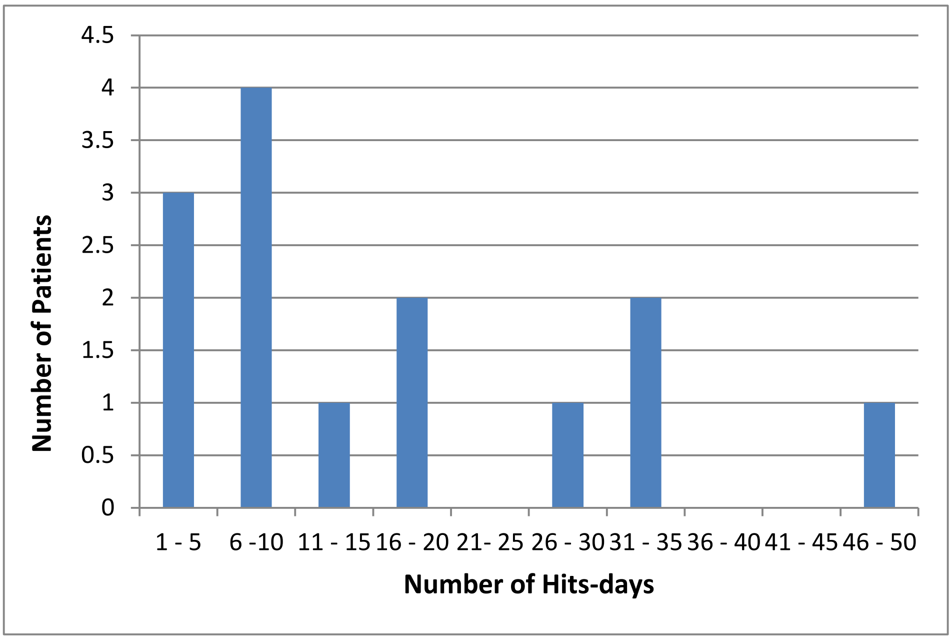


Figure 7.11: Use of M-Health App System. The Figure excludes one extreme observation where a patient had 61 hit-days.

7.7.7 Qualitative Study

The qualitative study conducted during the field study evaluation aimed at establishing how useful are mobile phone-based PHR systems to end-users including patients and healthcare givers. First, three focus group discussions were conducted toward the end of the field study. The focus group discussions contained five users each, for a total of 15 participants. The focus group discussions were held at the Faculty of Science and Technology (FoST), Uganda Christian University and lasted approximately one hour. The investigator facilitated all the focus group discussions, with the research assistant taking the field notes.

7.7.7.1 Analysis

We recorded all the three focus group discussion, and both video and audio data were archived for further review and analysis of usability problems. The recordings were automatically time stamped to facilitate tagging issues of concern. The issues and reactions of users could be easily compared. Finally, we conducted a thematic, inductive analysis of the interview transcripts.

We began by applying descriptive codes to phenomena that we saw arising in each discussion. We then iteratively clustered these codes into higher level category groupings until we arrived at the themes that are described in the next section.

7.7.8 Patients' Qualitative Assessment

During the focus group discussions with the patients, we observed that the attitude of patients toward M-Health App system was overwhelmingly positive. Participants derived seven categories of potential benefits of the M-Health App system: supporting their memory regarding information from the hospital, confirming personal health records and accuracy, learning more about their condition, healthcare coordination, support medical decision-making, increasing their participation in their care, and understanding clinical notes. In the next subsection, we describe these benefits in more details.

7.7.8.1 Memory Support

Of the 15 (fifteen) respondents who participated in this study, three-quarters reported that they used M-Health App system as a memory aid to confirm medication doses or test results, which they had difficulty in remembering. Similarly, participants commented that the M-Health App system provides an opportunity to remember much of the information that was conveyed during discharge. Thus, the records stored with M-Health App system will act as a reminder after the patient is discharged;

> *"... Whenever you are with the doctor at the clinic, there is so much information that is verbally communicated to you, which is absolutely impossible to process all the information. With M-Health App system, such information is stored on my mobile phone, which you can consult that day or even the next day..."*

7.7.8.2 Confirming Personal Health Records and Accuracy

The majority of participants observed that the M-Health App system assured them of being able to look up their results and confirm that their records are up to-date and accurate. In fact, over three-quarters of the participants liked the M-Health App system because it provides the ability to review their records for completeness and they are assured of confirming that their details were recorded accurately;

"... Using my airtime to download my health records to the mobile phone was not an issue to worry about. What interested me was the ability to check for completeness of my records and accuracy..."

7.7.8.3 Learning about their Conditions Regularly

The participants felt that accessing their records will help them learn about their health frequently. Additionally, participants reported that they will be able to get insights into the previous medication and management, which can support self-education and management of certain diseases. Participants also appreciated the fact that M-Health App system keeps track of previous treatment and medication;

"...The system enables me understand previous illness and possible causes, which allows me to say "oh, because of this, so I need to take care of myself such that it doesn't happen again...."

7.7.8.4 Supports Healthcare Coordination

All the participants agreed that providing access to their health records will improve their ability to participate in their healthcare. Participants reported that whenever they visit the facility for healthcare services, they are given paper notes describing their illness and medication, which are hard to keep. When they report back the next day for check-up or after a longer period of time for similar services, the healthcare practitioner usually looks for their paper-based files in a heap of files, which, in most cases, delays their treatment. The M-Health App system supports the provision of laboratory test results to their doctors. This helps to avoid duplication of test results among healthcare providers. Moreover, patients can also provide an exact copy of his record to the doctor, rather than looking up the paper-based file from a heap of files.

7.7.8.5 Supports Medical Decision-Making

The results from the focus group discussion further indicate that the M-Health App system provides transparency to healthcare decision-making. Participants liked the fact that they can follow and understand the treatment and medication processes described by the healthcare practitioner. Participants described that understanding these processes can bring a number of benefits: allowing them actively participate in their own healthcare, improve their communication with their healthcare practitioner and reassure them that they own the correct records from the right healthcare professional. Additionally, one participant noted that it also provides an opportunity to have a greater sense of control of their records, which has not been the case.

"...I think..... I have a much better understanding of the healthcare processes, which I feel I will be in more control and enables me to talk to the provider more freely..."

7.7.8.6 Understanding Clinical Notes

All the participants appreciated the fact that the M-Health App system eliminates the difficulty in reading and understanding medical jargon. Three participants noted that professional medical jargon were among the major reasons why they were not interested to keep the medical notes given to them.

"Previously,..... we could not understand those medical jargons. After completing the medication, there was no motivation to keep the medical notes. Even our children whom we have educated but not medical professionals could not understand these jargons…"

7.7.8.7 Increase Patients' Participation in their Healthcare

The majority of participants reported that the M-Health App system provide an opportunity to have access to their health records, which is likely to increase our participation in healthcare.

"...M-Health App system provides an opportunity to be more active and responsible with our healthcare. For example, the 'download my records' function enables me to regularly download and update my records, if am to provide a dependable and updated records to the provider. 'This is a great tool'…"

Similarly, all the participants agreed that the M-Health App system provides a great opportunity to have access to their records and thus increase the efficiency of getting their health information.

"...It is very easy to get an electronic copy of your records by yourself... this has motivated me to have a better phone that can support M-Health App system functionalities… "

7.7.9 M-Health App System Healthcare Professional Experience

Interesting to note is that, during the interviews after the trial period of field study, none of the participating healthcare professionals voiced any of the concerns that they mentioned during the focus group evaluation. In practice, none of the medical practitioners felt that the M-Health App system were problematic (confusing, overly time consuming, or embarrassed their patients) in any way. Instead, they recalled the M-Health App system in a positive light. For example, one nurse reported a patient who was concerned about the changes in medication using the M-Health App system documentation. In this case, the nurse explained the root cause of the changes, which was impossible before. Few patients (if not none) could consult their paper-based records.

All the participating healthcare professionals who had changed their documentation style to make it more understandable to patients did not view it as a problem, and none complained about the excessive time consuming to document the records.

> *"... It is not time consuming since it needs probably less than an hour. It's just adding a few sentences for every patient describing medication, history..., which makes it a little more interpretable..."*

One healthcare professional who changed the documentation style noted that it generated a positive outcome from patients who visited the healthcare centre for review. The patients could understand and refer to the previous medication, which brought harmony among medical practitioners to support the idea of facilitating patients access their health records.

To further asses the usefulness of M-Health App system on the healthcare centre, we interviewed two support staff in a single focus group. Each of the staff could not recall any question or interaction that was inappropriate or problematic;

> *"... All the patients were praising M-Health App system. At first, I did not know what the system is all about. But when a patient demonstrated it to me, I wished having similar system for my children..."*

7.8 M-Health App System Final Evaluation Session

At the end of the field study session, we also administered another reliable and valid measure, namely the Post-Study System Usability Questionnaire (PSSUQ) (Lewis, 1992), based on previous studies (Buchanan et al., 2001; Zheng, Padman, Johnson, & Diamond, 2005; Dabbs et al., 2009; Baltrunas, Ludwig, Peer, & Ricci, 2012). The PSSUQ was designed specifically for use at the completion of usability studies. It was used to assess the overall user satisfaction with 17 aspects of the system and the interfaces, using the same seven-point scale as the after-scenario Questionnaire (ASQ) (lower scores = higher satisfaction; possible range = 1-7).

Table 7.2 describes the Mean PSSUQ Scores after the Field Study ((M= mean score, SD = standard deviation). Compared to the previous paper-based solution, participants stated that the M-Health App system was easy and simple to use (1 ± 0), faster (1 ± 0), and resulted in higher quality data (1 ± 0). Additionally, participants felt that the M-Health App system facilitates their interaction with the healthcare provider (1 ± 0), and wished to continue using the system compared to the earlier paper-based system.

Table 7-2: Mean PSSUQ Scores after the Field Study (N=15). The PSSUQ scores range from 1-7 (lower scores = higher satisfaction).

	No of respondents for each option of a 7-point Likert scale								
	Strongly Agree				**Strongly disagree**				
	1	**2**	**3**	**4**	**5**	**6**	**7**	**N/A**	**M ± SD**
Questions (Compared with paper-based system)									
1. Easy to use system	15	0	0	0	0	0	0	0	1 ± 0
2. Simple to use system	15	0	0	0	0	0	0	0	1 ± 0
3. Effectively complete tasks and scenarios	15	0	0	0	0	0	0	0	1 ± 0
4. Quickly complete tasks and scenarios	15	0	0	0	0	0	0	0	1 ± 0
5. Efficiently complete tasks and scenarios	15	0	0	0	0	0	0	0	1 ± 0
6. Comfort to use the system	15	0	0	0	0	0	0	0	1 ± 0
7. Easy to learn to use system	15	0	0	0	0	0	0	0	1 ± 0
8. Believe could become Productive using system	15	0	0	0	0	0	0	0	1 ± 0
9. Error messages were clear	10	4	1	0	0	0	0	0	1.4 ±.63
10. Easily recover from mistakes	11	3	1	0	0	0	0	0	1.3± .62
11. Information about M-Health App was clear	15	0	0	0	0	0	0	0	1 ± 0
12. Easy to find needed information	15	0	0	0	0	0	0	0	1 ± 0
13. Easy to understand information	13	2	0	0	0	0	0	0	1.1±.35
14. Information helped complete the task	11	3	1	0	0	0	0	0	1.3±.62
15. Information was clearly organized	15	0	0	0	0	0	0	0	1 ± 0
16. Interface was pleasant	15	0	0	0	0	0	0	0	1 ± 0
17. Enjoyed using interface	15	0	0	0	0	0	0	0	1 ± 0
PSSUQ Overall	**15**	**12**	**3**	**0**	**0**	**0**	**0**	**0**	**1.06+.13**

Overall, the M-Health App was generally considered as both a nice-to-have and a need-to-have tool and participants would like to see it implemented in order to eliminate paper-based PHRs. Additionally, all participants expressed appreciation for the opportunity to be involved in the testing process

7.9 Summary

Our implementation of PHR system distributed on mobile phones remains one of the largest patient-centric systems for people living in rural areas of developing countries. The PHR system enables patients to securely download and update their medical records onto the mobile phone and share the records with healthcare providers in an offline mode i.e. when hospital servers are offline due to unstable main electricity and/or unreliable Internet connection. In performing the evaluation of our system, we have established two key contributions;

- Mobile phones can be used to provide efficient and secure storage of PHRs to people leaving in rural areas of developing countries.
- Suitably adapted PHR system can address health needs of low-literacy and technology-constrained users in developing countries.

"Obstacles are only frightening when you take your eyes off the goal."

- *Henry Ford*

CHAPTER 8: SUMMARY, CONCLUSIONS, LIMITATIONS AND FUTURE DIRECTIONS

8. Introduction

This chapter is organised into four sections. The first section revisits the research problem and the research questions, highlighting how each of the research questions was answered. The second section contains the conclusions arising from the study process as well as the evaluation results of the system developed. Additionally, the section also highlights the contributions of this study. The third section covers limitations of the study whereas the fourth presents possible directions for future work.

8.1 Revisiting the Research Problem

This research was framed within the research area of ICT4D, aimed at empowering patients to own their Personal Health Records (PHRs) on mobile phones, since mobile phones are ICT tools that the majority of people living in developing countries own. Additionally, a systematic review of literature has revealed that while Electronic Health Record (EHR) systems can greatly address the challenges facing healthcare systems in developing countries, the majority of EHR systems are designed for developed countries and cannot be adapted for implementation in developing countries. The failure of adoption is attributed to many factors including: the majority of EHR systems are developed with the user contexts in the developed world and thus do not represent the needs of the users in developing world. Additionally, current EHR systems support only online access control authorities. When the server fails, for example, due to frequent power outages that is common in developing countries, access control decisions cannot be made, making patients' health records unreachable.

Previous studies by Mechael (2009), Kaplan (2006), and Blaya, Fraser, and Holt, (2010) demonstrate that in order for the EHR systems to satisfy the intended users, specifically in developing countries, existing EHR systems need to be extended on mobile phones such that records can be made available when hospital servers are offline. This reduces the need to rely on online access control authorities in the provision of PHRs.

While mobile phones offer storage capabilities to users, and can provide offline access of Personal Health Records (PHRs), they generally do not provide sufficient security mechanism to protect the data to which users operate on. Therefore, the main research question of this study was: Can personal health records be stored securely and usefully on mobile phones? To answer this question, the following specific research questions were required;

RQ1. Can I provide an access control architecture that can be used to protect patient's records on mobile phone?

RQ2. Can the proposed architecture be usable on mobile phone without interfering with the 'normal' use of the device in terms of its efficiency, performance and resource management?

RQ3. How useful are the mobile phone-based PHR systems to the users including healthcare professionals and the patients?

These research questions were answered through an analysis of patients' needs and requirements, and later on design an access control framework that protects personal health records on mobile phone. The thesis describes the design and implementation of the mobile phone-based PHR system using the four-stage process of Patient-Centred Design (PCD) approach: (1) Analysis, (2) planning, (3) Implementation and (4) evaluation. The participatory design approach to design was used in combination with Human Access Points (HAP) technique since majority of patients were low technology literacy, and thus needed persons in the community who are more knowledgeable about the potential of the technology to design the system.

The first stage of Patient-Centred Design approach (analysis, fact finding and conceptualisation), reported in chapter four, investigated the current state of practices of healthcare service provision, and personal health records in particular. This enabled the identification of challenges and opportunities for developing mobile phone-based PHR system, as well as refining the research problem.

The study revealed that providing efficient and timely access to healthcare services was indeed a difficult task. The PHR practices were primarily paper-based. This imposes many disadvantages, such as unavailability and loss of patient information, delays in accessing the information and space limitation for record-keeping. Additionally, due to infrastructural constraints, such as intermittent power and Internet connectivity, the introduction of the healthcare information system (Clinic Master) to automate healthcare processes had received a great challenge. In most cases, Clinic Master was not useful due to frequent power outages and unreliable Internet connections.

The second PCD stage – planning – described participatory design and paper prototyping activities with the community representatives who are more knowledgeable about the potential of the technology. The purpose was to develop detailed requirement specifications for the design of an access control framework (ACOF) that protects personal health information on mobile phone (RQ1). Similarly, the formative evaluation conducted with the final beneficiaries of the technology re-affirm that Human Access Points (HAP) can be used to reveal end-user needs and requirements, as well as testing the initial prototypes.

The third PCD stage – implementation – detailed the implementation of the mobile phone-based PHR system called the M-Health App system. Contrary to the previous approaches, our system enable patients to securely download and update their medical records onto the mobile phone and share their records with healthcare providers in an offline mode; i.e. when hospital servers are offline due to unstable main electricity and/or unreliable Internet connection. To enable offline access, the developed mobile application incorporates the "push model" where patients can periodically download and update their health records to the mobile phone with minimal user intervention. Once the encrypted records are downloaded to the mobile phone, the application then breaks down the records into an XML hierarchical structure such that records can be viewed/shared selectively. However, only users with a PIN that satisfies the policy are able to decrypt the records. A key advantage of the M-Health App system is that it minimises the need to rely on centralised databases, which require constant power supply and Internet connectivity. As noted earlier, power failures and bandwidth limitations make standard EHR implementations problematic to run in the developing world.

The final PCD stage – evaluation – reported results from laboratory evaluations: performance evaluation, storage overhead evaluation, waiting time evaluation, Heuristic Evaluation, user experience evaluation and focus group evaluation (RQ2), and field study-based evaluation of the M-Health App system (RQ3). As described in sections 7.2, 7.3.2 and 7.5, standard guidelines and procedures were used to evaluate the M-Health App system for performance and usability evaluations. Every stage of PCD included testing and analysis, and these activities required to loop back to the earlier stages so that development occurs in iterative cycles of assessing-designing-testing-analysing-refining-testing-analysing-refining (Nielsen, 1993).

The results of the laboratory evaluation show that the proposed Identity-Based Encryption (IBE)-inspired architecture can be used on the mobile phone without interfering with the 'normal' use of the device in terms of its efficiency, performance and resource management (RQ2). Once patients' records are encrypted by the healthcare server, the encrypted records can be downloaded onto the patient's mobile phone for portability and offline access. The waiting time (time taken to decrypt the records on the mobile phone, and time taken to download the records (using 3G and WLAN) from the server to the mobile phone) is within the acceptable range (Nielsen, 1997; Zona, 1999). Additionally, the results of the field study show that M-Health App system was useful and satisfied most of the users including patients and healthcare givers (RQ3). In fact, the head of the clinical officers reported that they have communicated to their higher authority requesting for the M-Health App system to be incorporated into the daily operation of the healthcare services. Actually, the M-Health App system encouraged patients to check for the accuracy of their records, support decision-making, and coordination of healthcare. The healthcare givers reported that the M-Health App system supports the provision of EHRs when the healthcare server is offline. This reduces the need to rely on server-based access control authorities in the provision of personal health records. Further conclusions arising from the study are given in the next section.

8.2 Conclusion

This study contributes key findings to the literature on the outcomes of providing patients access to mobile phone-based health records. At the start of the study, patients were uniformly positive about the idea of empowering them own their health records on mobile phones, due to the fact that the majority of the patients were using paper-based records that are characterised by loss of information and delay in accessing healthcare services. Patients reported that the M-Health App system had a number of practical uses in managing and promoting quality healthcare. Medical jargon in paper-based health records was an impediment to patients understanding their health records. The M-Health App system effectively eliminated the problem of not reading and understanding their records. Although healthcare givers initially expressed concerns towards mobile phone-based records, after the trial period, none of these concerns materialised. Medical practitioners viewed mobile phone-based patient-accessible records much more favourably than paper-based records. The only persistent concern voiced by any of the medical practitioners was whether increasing online updates of health information by patients will not increase medical errors, since the majority of the patients may not know what to add or remove. As a result, medical practitioners suggested that patients should be given read only access in order to minimise medical errors.

While User-Centred Design is highly acclaimed as a means of ensuring end-user acceptability, its application with patient users has not been widely disseminated to the healthcare technology disciplines despite calls for its application (Gustafson et al., 1999; IOM, 2001). As described in section 3.16.2, this gap is problematic since healthcare givers and technology developers normally identify the health problems and propose possible interventions, which many of them are intended for use by patients. In this study, a patient-centric PHR system has been presented. The main design objectives were;

- Enable patients participate fully in the design and testing of an interactive PHR system
- Minimize the Internet connectivity requirement of the mobile PHR user (following the health record's download, Internet coverage is not further required as the PHR execute on standalone mode, patients should return online only to update their health records)
- Cater for future PHR updates based on a ''push model'', wherein new personal health record content is pushed to the mobile terminal with minimal user intervention as soon as it is added by the hospital administrator to the back-end server.

The proposed M-Health App system relies on Java and XML technologies for enhanced efficiency, interoperability and compatibility with the E-Health content standards. Implementation experiences re-affirm that J2ME and jpair library offers an ideal platform for the development of powerful, interactive and secure PHR applications tailored to handset devices with restricted processing, memory and storage resources.

Keeping our focus on the tasks and users throughout the development process helped reduce the risk of designing an interactive PHR system that was based entirely on what we considered important and useful rather than what the patient thought would assist with self-management activities. As previous studies have shown, involving users throughout the entire development process ensures that the final technology is functional and acceptable as soon as it is ready to be deployed. Based on our results, we re-affirm that applying Patient-Centred Design to the development of an interactive PHR system intended for use by the patients will assure that users' needs and expectations are met.

The hierarchical structuring and display of personal health records was found useful by the majority of patients. The hierarchical structuring enables patients to selectively share their health records. The structuring was proposed and designed by the Human Access Points (HAP) during the participatory design process (co-design). This re-affirms the importance of Human Access Points (HAP) in bridging the literacy gap in the participatory design process. Additionally, using face-to-face interviews, we were able to probe the attitude of patients and medical practitioners, both before and after implementation, in more depth than in previous studies.

The study was also able to provide detailed information on the frequency of use of the M-Health App system by patients. The server log files demonstrate that the use of M-Health App System was higher than PCASSO uses (Masys, Baker, Butros, & Cowles, 2002). Because our population consisted of patients with low technology and literacy levels, we had expected use to be much lower than what was observed. Among users, the median number of hit-days was higher than the mean number of hospital visits. This suggests that patients did consult M-Health App system repeatedly between visits.

To turn to the theoretic contribution of this study, an extensive access control framework that protects patients' health records was presented (section 6.4). In contrast to other architectures, the framework is designed to enable secure export of PHRs beyond the hospital's server security domain. This includes personal health records that are held by patients on mobile phones. To protect the exported records, our framework provides end-to-end encryption, and content-based access control. A summary of the key advantages of the proposed framework to rural healthcare are given in section 6.14, chapter six.

Overall, this study concludes that, understanding patients and healthcare givers' expectations, attitude and needs in the design process of the PHR system is a key to developing a usable and useful PHR system. The results of the evaluation (sections 7.3, 7.6, and 7.7) demonstrate that mobile phones can be used to provide efficient and secure storage of PHRs in the developing countries. Participants (patients and healthcare givers) considered our system as a nice-to-have and a need-to-have system, and majority of participants would like to see it implemented in order to eliminate the difficulties of paper-based PHR systems. Furthermore, the patients prefer M-Health App system over the current paper-based system because of the following reasons;

- Confirms Personal Health Records (PHRs) for accuracy
- Enables to understand clinical notes and laboratory results
- Supports healthcare coordination

- Supports medical decision making
- Increase their participation in their healthcare
- Support their memory

Similarly, none of the medical practitioner reported any problem during the use of M-Health App. Instead, they recalled the M-Health App system in a positive light: supports continuity when the server is offline, and improves their relationship with the patients.

8.3 Limitations of the Study

There are number of attributes that validates the outcome of the research studies. For example, sample selection, validity of participant samples, the data collected, and the generalisation of the results (Mugwanya, 2013).

In the case of this study, the M-Health App system was designed and evaluated in an academic subspecialty practice that may not be representative of most practice settings. The majority of the patient population enjoyed a higher level of knowledge of mobile phone experiences, which may not be the case to the general population. Furthermore, since the field study was conducted for only three months – due to the limited resources, and the context of a PhD study that involves limited time, patients and healthcare giver satisfaction could have increased (due to increased familiarity) or decreased (due to fading of initial enthusiasm) if the study was carried out over a longer period of time

Like in the majority of previous studies, much of the data were qualitative. While this can provide an accurate description of the experiences of those involved in the design and evaluation of the intervention, these data cannot quantify or statistically compare differences in healthcare experiences.

Lastly, we noted that the field study sample size (n = 15) was smaller due to the limited resources such as mobile phones to the patients. As such, we were unable to collect information from patients who were eligible for the study but did not participate. These patients may be different, biasing the results of the field study. A larger sample would have provided a more precise estimate of effect.

8.4 Directions for Future Work

As already highlighted in the limitations of this study, the small size of the field study sample, and the short duration of the trial are not adequate to assess effectively the outcomes of M-Health App system. The benefits and usefulness reported by M-Health App users could potentially translate into improved medical and PHR outcomes. As mobile phone penetration in developing countries progresses, and initiatives to increase collaborative decision-making between patients and healthcare givers increase, we anticipate there will be more interest in providing patients accesses their medical records using mobile phones. The findings (described in sections 7.7.8 and 7.7.9) suggest a number of potential benefits, and few if any adverse consequences to providing this access. Therefore, studies involving larger numbers of more patients and clinical settings will be necessary to further evaluate the impact of M-Health App system.

8.5 Assessing the Impact of M-Health App System

As already highlighted in the limitations of this study, the field study evaluation of this study was limited by time and other resources. However, the study has set the stage from where more field evaluations and analysis of M-Health App system can be done. From these, more insightful observations could emerge. For example, it would be important to investigate the usefulness of M-Health App system when converted into a local language (Luganda).

8.6 Further Development Efforts

In the development of the M-Health App system, jpair did not allow faster decryption of the records stored on the Huawei Ideos phones. Enabling faster decryption of the records can increase user satisfaction among end-users including patients and healthcare providers. This can be further investigated.

8.7 References

[1] "Standard Of Living Definition". Investopedia.com. [Accessed: 11-03-2013], from http://www.investopedia.com/terms/s/standard-of-living.asp#ixzz1VULi2yEI.

[2] “Glocal” eHealth Policy: From Silos to Systems. [Accessed: 02/08/2012], from http://www.rockefellerfoundation.org/uploads/files/3af08a9f-a1a4-4fd5-9376-9b0bd498ceac-silos-to.pdf.

[3] Abdalla, M., & Pointcheval, D. (2005). Simple password-based encrypted key exchange protocols. In *Topics in cryptology–CT-RSA 2005* (pp. 191-208). Springer Berlin Heidelberg.

[4] Abdul, S.S. (2008). The challenges, problems and strategies of electronic medical record implementation: A case study of an eye hospital from India. Master’s thesis, University of Tromso, Norway.

[5] Abras, C., Maloney-Krichmar, D and Preece, J. (2004). User-centred design. In *Encyclopedia of Human Computer Interaction*, W. Bainbridge, Ed. Thousand Oaks: Sage Publications.

[6] Adesina, A. O., Agbele, K. K., Februarie, R., Abidoye, A. P., Nyongesa, H. O., Cape, W., & Adesina, A. (2011). Ensuring the security and privacy of information in mobile health-care communication systems. *S Afr J Sci*, *107*(9/10), 26-32.

[7] Adida, B., & Kohane, I. S. (2006). GenePING: secure, scalable management of personal genomic data. *BMC genomics*, *7*(1), 93.

[8] Adida, B., Sanyal, A., Zabak, S., Kohane, I. S., & Mandl, K. D. (2010). Indivo x: developing a fully substitutable personally controlled health record platform. In *AMIA Annual Symposium Proceedings* (Vol. 2010, p. 6). American Medical Informatics Association.

[9] Aggarwal, M., & Vennon, T. (2010). *Study of BlackBerry proof-of-concept malicious applications*. Technical Report White paper, SMobile Global Threat Center.

[10] Akdeniz, Y. Cryptography & Encryption. (August 1996). Cyber-Rights & Cyber-Liberties (UK) [Accessed 27th May 2013], from http://www.leeds.ac.uk/law/pgs/yaman/cryptog.htm.

[11] Akinyele, J. A., Pagano, M. W., Green, M. D., Lehmann, C. U., Peterson, Z. N., & Rubin, A. D. (2011, October). Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 75-86). ACM.

[12] Als .B .S, Jensen .J .J, & Skov .M .B (2005): *Comparison of think-aloud and constructive interaction in usability testing with children.* In Proceedings of the International conference on Interaction design and children *(IDC '05).* ACM, New York, NY, USA, pp 9-16.

[13] Android developer reference. [Accessed: 08/10/2013], from http://developer.android.com/training/articles/perf-tips.html.

[14] Anokwa, Y. (2010). Delivering Better HIV Care in Sub-Saharan Africa Using Phone-Based Clinical Summaries and Reminders. [Accessed: 12\03\2012], from http://anokwa.com/publications/2010_UW_Generals_Paper.pdf.

[15] Anokwa, Y., Allen, C., & Parikh, T. (2008). Deploying a Medical Record System in Rural Rwanda. *HCI for Community and International Development at CHI*, *2008*.

[16] Anokwa, Y., Ribeka, N., Parikh, T., Borriello, G., & Were, M. C. (2012, March). Design of a phone-based clinical decision support system for resource-limited settings. In *Proceedings of the Fifth International Conference on Information and Communication Technologies and Development* (pp. 13-24). ACM.

[17] Antón-Rodríguez, M., de la Torre-Díez, I., Gutiérrez-Díez, P., Díaz-Pernas, F. J., Martínez-Zarzuela, M., González-Ortega, D., & Díez-Higuera, J. F. (2011, January). Mobile Access System for the Management of Electronic Health Records of Patients with Mental Disability. In *International Symposium on Distributed Computing and Artificial Intelligence* (pp. 329-336). Springer Berlin Heidelberg.

[18] Arhippainen, L., & Tähti, M. (2003, December). Empirical evaluation of user experience in two adaptive mobile application prototypes. In *Proceedings of the 2nd international conference on mobile and ubiquitous multimedia* (pp. 27-34).

[19] Array Networks Inc. SSL VPN vs IPSec VPN, Jan. 2003. White paper.

[20] ASTM E31.28, Continuity of Care Record (CCR): the concept paper of the CCR. [Accessed 16/05/2013], from www.astm.org/COMMIT/E31_ConceptPaper.doc.

[21] ASTM International. ASTM E2369 - 05e1 Standard Specification for Continuity of Care Record (CCR), 2009

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

[23] Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2012, January). Novel Anti-forensics Approaches for Smart Phones. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 5424-5431). IEEE.

[24] Bahga, A., & Madisetti, V. K. (2013). A Cloud-Based Approach to Interoperable EHRs. [Accessed: 17-10-2013], from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6497443

[25] Bailey, B. (2001). Acceptable computer response times. UI Design Update Newsletter, April 2001. [Accessed: 23/09/2013] from http://www.humanfactors.com/downloads/apr012.htm#bobbailey.

[26] Baker, D. B., & Masys, D. R. (1999). PCASSO: a design for secure communication of personal health information via the Internet. *International journal of medical informatics*, *54*(2), 97-104.

[27] Baltrunas, L., Ludwig, B., Peer, S., & Ricci, F. (2012). Context relevance assessment and exploitation in mobile recommender systems. *Personal and Ubiquitous Computing*, *16*(5), 507-526.

[28] Barka, E., Boulmalf, M., Alteniji, A., Al Suwaidi, H., Khazaimy, H., & Al Mansouri, M. (2006, November). Impact of Security on the Performance of Wireless-Local Area Networks. In *Innovations in Information Technology, 2006* (pp. 1-5). IEEE.

[29] Barnes, S. J., & Scornavacca, E. (2004). Mobile marketing: the role of permission and acceptance. *International Journal of Mobile Communications*, *2*(2), 128-139.

[30] Bederson, B. B., Clamage, A., Czerwinski, M. P., & Robertson, G. G. (2003, April). A fisheye calendar interface for PDAs: Providing overviews for small displays. In *CHI'03 extended abstracts on Human factors in computing systems* (pp. 618-619). ACM.

[31] Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009, November). Patient controlled encryption: ensuring privacy of electronic medical records. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 103-114). ACM.

[32] Benbasat, I., & Weber, R. (1996). Research commentary: Rethinking "diversity" in information systems research. *Information systems research*, *7*(4), 389-399.

[33] Benelli, G. & Pozzebon, A. (2010). Near field communication and health: Turning a mobile phone into an interactive multipurpose assistant in healthcare scenarios. *In Biomedical Engineering Systems and Technologies, International Joint Conference, BIOSTEC 2009*, Revised Selected Papers, volume 52 of Communications in Computer and Information Science, pages 356-368. Springer.

[34] Bernstein, W. S., Murchinson, J., V., Dutton, M., J., Keville, D., T., Belfort, R., D. (2008). Whose data is it anyway? Expanding consumer control over personal health information," *California Healthcare Foundation: Issue Brief.*

[35] Bevan, N., & Curson, I. (1999). Planning and implementing user-centred design. CHI ’99 extended abstracts on human factors in computer systems, 137–138.

[36] Beyer, H., & Holtzblatt, K. (1999). Contextual design. *interactions*, *6*(1), 32-42.

[37] Bhatnagar, S. (1992). Information Technology and Socio-Development: Some strategies for developing countries. *Social implications of computers in developing countries*, 1-9.

[38] Bittau, A., Handley, M., & Lackey, J. (2006, May). The final nail in WEP's coffin. In *Security and Privacy, 2006 IEEE Symposium on* (pp. 15-pp). IEEE.

[39] Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., ... & Sheikh, A. (2011). The impact of eHealth on the quality and safety of health care: a systematic overview. *PLoS medicine*, *8*(1), e1000387.

[40] Blake, I. F., Seroussi, G., & Smart, N. (1999). *Elliptic curves in cryptography* (Vol. 265). Cambridge University Press.

[41] Blaya, J. A., Fraser, H. S., & Holt, B. (2010). E-health technologies show promise in developing countries. *Health Affairs*, *29*(2), 244-251.

[42] Boehner, K., Vertesi, J., Sengers, P., & Dourish, P. (2007, April). How HCI interprets the probes. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 1077-1086). ACM.

[43] Boneh, D., & Franklin, M. (2001, January). Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin Heidelberg.

[44] Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC health services research*, *10*(1), 231.

[45] Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, *6*(4), 260-279.

[46] Bouch, A., Kuchinsky, A., & Bhatti, N. (2000, April). Quality is in the eye of the beholder: meeting users' requirements for Internet quality of service. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 297-304). ACM.

[47] Boulmalf, M., Barka, E., & Lakas, A. (2007). Analysis of the effect of security on data and voice traffic in WLAN. *Computer Communications*, *30*(11), 2468-2477.

[48] Braa, J. & Blobel, B. (2003) Strategies for developing health information systems in developing countries. In D. Khakhar (Ed.), WITFOR 2003 White Book (pp. 175–219). Laxenburg, Austria, IFIP Press.

[49] Braa, J., & Hedberg, C. (2002). The struggle for district-based health information systems in South Africa. *The information society*, *18*(2), 113-127.

[50] Brewster, S., & Dunlop, M. (Eds.). (2004). *Mobile Human-Computer Interaction-Mobile HCI 2004: 6th International Symposium, Glasgow, UK, September 13-16, 2004, Proceedings* (Vol. 3160). Springer.

[51] Brodie, M., Flournoy, R. E., Altman, D. E., Blendon, R. J., Benson, J. M., & Rosenbaum, M. D. (2000). Health information, the Internet, and the digital divide. *Health affairs*, *19*(6), 255-265.

[52] Buchanan, G., Farrant, S., Jones, M., Thimbleby, H., Marsden, G., & Pazzani, M. (2001, April). Improving mobile Internet usability. In *Proceedings of the 10th international conference on World Wide Web* (pp. 673-680). ACM.

[53] Buyukkokten, O., Kaljuvee, O., Garcia-Molina, H., Paepcke, A., & Winograd, T. (2002). Efficient web browsing on handheld devices using page and form summarization. *ACM Transactions on Information Systems*, *20*(1), 82-115.

[54] California Healthcare Foundation. (2008). Whose data is it anyway? Expanding consumer control over personal health information. California Healthcare Foundation: Issue Brief. [Accessed on 11/05/2013] from http://www.oregon.gov/OHA/OHPR/HIIAC/WebOnlyMaterials/WhoseDataIsItAnywayIB.pdf

[55] Canadian Heritage Information Network (CHIN) (2004): Tip sheets, personal digital assistants (PDA), PDA aesthetics and interface design, creating and managing digital content. [Accessed: 02/11/2011, from http://www.chin.gc.ca/English/Digital_Content/index.html.

[56] Card, S. K., Moran, T. P., & Newell, A. (1980). The keystroke-level model for user performance time with interactive systems. *Communications of the ACM*, *23*(7), 396-410.

[57] Carpenter, I., Ram, M. B., Croft, G. P., & Williams, J. G. (2007). Medical records and record-keeping standards. *Clinical Medicine*, *7*(4), 328-331.

[58] Certification Commission for Health Information Technology (CCHIT). [Accessed: 30-10-2011], from http://www.cchit.org/

[59] Chadwick, D. (1999). Smart Cards aren't always the Smart Choice. *Computer*, *32*(12), 142-143.

[60] Chandrasekhar, C.P. & Ghosh, J (2001). Information and communication technologies and health in low income countries: the potential and the constraints, Bulletin of the World Health Organization, Vol. 79 No. 9, pp. 850-5.

[61] Chang, K. (2012). *Security and Collaboration Protocols for Mobile and Sensor Networks* (Doctoral dissertation, The University of Michigan).

[62] Chepken, C. (2012). *Telecommuting in the Developing World: A Case of the Day-Labour Market* (Doctoral dissertation, DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF SCIENCE, UNIVERSITY OF CAPE TOWN).

[63] Chib, A., Lwin, M. O., Ang, J., Lin, H., & Santoso, F. (2008). Midwives and mobiles: using ICTs to improve healthcare in Aceh Besar, Indonesia 1. *Asian Journal of Communication*, *18*(4), 348-364.

[64] Chinn, M. D., & Fairlie, R. W. (2010). ICT use in the developing world: an analysis of differences in computer and Internet penetration. *Review of International Economics*, *18*(1), 153-167.

[65] Chittaro, L., & Dal Cin, P. (2002). Evaluating interface design choices on WAP phones: Navigation and selection. *Personal and Ubiquitous Computing*, *6*(4), 237-244.

[66] Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *Journal of Medical Systems*, *30*(1), 57-64.

[67] Ciavarella, C., & Paternò, F. (2003). Design criteria for location-aware, indoor, PDA applications. In *Human-Computer Interaction with Mobile Devices and Services* (pp. 131-144). Springer Berlin Heidelberg.

[68] Citizenship and Immigration Canada. Tracking Public Perceptions of Biometrics, 2003. [Accessed Jan 13, 2011] from http:// www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf.

[69] Clason, D. L., & Dormody, T. J. (1994). Analyzing data measured by individual Likert-type items. *Journal of Agricultural Education*, *35*, 4.

[70] Coble, J. M., Maffitt, J. S., Orland, M. J., & Kahn, M. G. (1995). Contextual inquiry: discovering physicians' true needs. In *Proceedings of the Annual Symposium on Computer Application in Medical Care* (p. 469). American Medical Informatics Association.

[71] Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In IMA Int. Conf., pages 360-363.

[72] Cohn, S. P. (2006). Privacy and confidentiality in the nationwide health information network. [Accessed: 12-05-2013], from http://www.ncvhs.hhs.gov/060622lt.htm.

[73] Coleman, A. (2010). *Developing an e-health framework through electronic healthcare readiness assessment*. Doctoral Thesis. Nelson Mandela Metropolitan University. [Accessed: 10/08/2012], from http://www.nmmu.ac.za/documents/theses/Alfred%20Coleman.pdf.

[74] Cooper, A., & Reinmann, R. About Face 2.0 The essentials of interaction design, 2003. *New York: Wliey*.

[75] Cross, M. (2000). Europe's wrestling with electronic patient record. *Document world*, *5*(1), 30-33.

[76] Dabbs, A. D. V., Myers, B. A., Mc Curry, K. R., Dunbar-Jacob, J., Hawkins, R. P., Begey, A., & Dew, M. A. (2009). User-centered design and interactive health technologies for patients. *Computers, informatics, nursing: CIN*, *27*(3), 175.

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

[78] Dagorn, N., Bernard, N., & Varrette, S. (2005, July). Practical authentication in distributed environments. In *IEEE International Computer Systems and Information Technology Conference (ICSIT'05)* (Vol. 1, pp. 19-21).

[79] Dalle, J. M. & Jullien, N. (2002). *Open-Source vs. Proprietary Software.* Working paper. [Accessed: 17-04-2012], from www.flosshub.org/system/files/dalle2.pdf.

[80] De Klerk, A. (1992). The right of patients to have access to their medical records: the position in South African law. *Medicine and law*, *12*(1-2), 77-83.

[81] De Mul, M., & Berg, M. V. D. (2007). Completeness of medical records in emergency trauma care and an IT-based strategy for improvement. *Informatics for Health and Social Care*, *32*(2), 157-167.

[82] Dell, N., & Borriello, G. (2013, January). Mobile tools for point-of-care diagnostics in the developing world. In *Proceedings of the 3rd ACM Symposium on Computing for Development* (p. 9). ACM.

[83] Deluca, J.M., & Enmark, R. (2002). *The CEO's Guide to Healthcare Information Systems,* John Wiley & Sons, Inc., San Francisco, CA.

[84] Demiris, G., Afrin, L. B., Speedie, S., Courtney, K. L., Sondhi, M., Vimarlund, V., ... & Lynch, C. (2008). Patient-centered applications: use of information technology to

promote disease management and wellness. A white paper by the AMIA knowledge in motion working group. *Journal of the American Medical Informatics Association*, *15*(1), 8-13.

[85] Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. (2010, April). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 917-926). ACM.

[86] Detmer, D., Bloomrosen, M., Raymond, B., & Tang, P. (2008). Integrated personal health records: transformative tools for consumer-centric care. *BMC medical informatics and decision making*, *8*(1), 45.

[87] Dickinson, G., Fischetti, L., & Heard, S. (2004). HL7 EHR System Functional Model Draft Standard for Trial Use. *Health Level*, *7*. [Accessed: Accessed 15/05/2013], from from http://www.hl7.org/documentcenter/public_temp_9ACD89C2-1C23-BA17-0C2AF73254CF80F1/wg/ehr/HL7_EHR-S_DSTU.pdf

[88] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, *22*(6), 644-654.

[89] Ding, Q., Pang, J., Fang, J., & Peng, X. U. (2007). Designing of chaotic system output sequence circuit based on FPGA and its applications in network encryption card. *Int J Innov Comput Inform Control*, *3*(2), 449-456.

[90] Dmitrienko, A., Hadzic, Z., Löhr, H., Sadeghi, A. R., & Winandy, M. (2013). Securing the access to electronic health records on mobile phones. In *Biomedical Engineering Systems and Technologies* (pp. 365-379). Springer Berlin Heidelberg.

[91] Dmitrienko, A., Hadzic, Z., Löhr, H., Winandy, M., & Sadeghi, A. R. (2011). A Security Architecture for Accessing Health Records on Mobile Phones. In *HEALTHINF* (pp. 87-96).

[92] Dolin, R. H., Alschuler, L., Beebe, C., Biron, P. V., Boyer, S. L., Essin, D., ... & Mattison, J. E. (2001). The HL7 clinical document architecture. *Journal of the American Medical Informatics Association*, *8*(6), 552-569.

[93] Dong, C. (2010). Jpair: A Quick Introduction. [Online] Available: https://personal.cis.strath.ac.uk/changyu.dong/jpair/intro.html [Accessed: 29-03-2012].

[94] Donner, J. (2006). The Social and Economic Implications of Mobile Telephony in Rwanda: An Ownership/Access Typology, Knowledge, Technology, & Policy, 19, 2, 17-28.

[95] Dossia. [Accessed: 01/09/2011], from http://dossia.org.

[96] Dudeck, J. (1998). Aspects of implementing and harmonizing healthcare communication standards. *International journal of medical informatics*, *48*(1), 163-171.

[97] Dunlop, M., & Brewster, S. (2002). The challenge of mobile devices for human computer interaction. *Personal and ubiquitous computing*, *6*(4), 235-236.

[98] Dwivedi, A., Bali, R. K., Belsis, M. A., Naguib, R. N. G., Every, P., & Nassar, N. S. (2003, April). Towards a practical healthcare information security model for healthcare institutions. In *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on* (pp. 114-117). IEEE.

[99] Eason, K. (1987). Information technology and organizational change. London: Taylor and Francis.

[100] Economist (2008). The Limits of Leapfrogging. [Accessed: 12-03-2013], from http://www.economist.com/opinion/displaystory.cfm?story_id=10650775

[101] Ekler, P., Nurminen, J. K., & Kiss, A. (2008, January). Experiences of implementing BitTorrent on Java ME platform. In *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE* (pp. 1154-1158). IEEE.

[102] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *Information Theory, IEEE Transactions on*, *31*(4), 469-472.

[103] Endsley, S., Kibbe, D. C., Linares, A., & Colorafi, K. (2006). An introduction to personal health records. *Family practice management*, *13*(5), 57.

[104] Etzioni, A. (2010). Personal health records: Why good ideas sometimes languish, *Issues in Science and Technology, vol. 26, no. 4*, pp. 59 – 66.

[105] EU. (2009). Office of the Data Protection Commissioner. EU Directive 95/46/EC: The data protection directive. [Accessed 12th May 2011] from http://www.dataprotection.ie/viewdoc.asp?DocID=92.

[106] Faridi, Z., Liberti, L., Shuval, K., Northrup, V., Ali, A., & Katz, D. L. (2008). Evaluating the impact of mobile telephone technology on type 2 diabetic patients' self-management: the NICHE pilot study. *Journal of evaluation in clinical practice*, *14*(3), 465-469.

[107] Ferguson, N., & Schneier, B. (2003). *Practical cryptography* (Vol. 141). New York: Wiley.

[108] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 224-274.

[109] Ferranti, J. M., Musser, R. C., Kawamoto, K., & Hammond, W. (2006). The clinical document architecture and the continuity of care record: a critical analysis. *Journal of the American Medical Informatics Association*, *13*(3), 245-252.

[110] Fiat, A & Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. In CRYPTO, pages 186-194.

[111] Fiore-Silfvast, B., Hartung, C., Iyengar, K., Iyengar, S., Israel-Ballard, K., Perin, N., & Anderson, R. (2013, January). Mobile video for patient education: the midwives' perspective. In *Proceedings of the 3rd ACM Symposium on Computing for Development* (p. 2). ACM.

[112] FIS' HealthManager. [Accessed: 31/08/2011], from http://www.fisglobal.com/products-healthcare-consumerdrivenhealthcare-healthmanager.

[113] Frampton, S. B., Gilpin, L., & Charmel, P. A. (2003). *Putting patients first: Designing and practicing patient-centered care*. San Francisco: Jossey-Bass.

[114] Fraser, H. S., Allen, C., Bailey, C., Douglas, G., Shin, S., & Blaya, J. (2007). Information systems for patient follow-up and chronic management of HIV and tuberculosis: a life-saving technology in resource-poor areas. *Journal of medical Internet research*, *9*(4).

[115] Fraser, H. S., Biondich, P., Moodley, D., Choi, S., Mamlin, B. W., & Szolovits, P. (2005). Implementing electronic medical record systems in developing countries. *Informatics in primary care*, *13*(2), 83-96.

[116] Fridsma, D. B., Ford, P., & Altman, R. (1994). A survey of patient access to electronic mail: attitudes, barriers, and opportunities. In *Proceedings of the annual symposium on computer application in medical care* (p. 15). American Medical Informatics Association.

[117] Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. *Computers & Security*, *19*(6), 529-539.

[118] Gagnon, M. P., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y., Duplantie, J., ... & Légaré, F. (2009). Users' perspectives of barriers and facilitators to implementing EHR in Canada: A study protocol. *Implementation Science*, *4*(1), 20.

[119] Garets, D., & Davis, M. (2006). Electronic medical records vs. electronic health records: yes, there is a difference. *Policy white paper. Chicago, HIMSS Analytics*.

[120] Garrido, T., Jamieson, L., Zhou, Y., Wiesenthal, A., & Liang, L. (2005). Effect of electronic health records in ambulatory care: retrospective, serial, cross sectional study. *Bmj*, *330*(7491), 581.

[121] Garson, K., & Adams, C. (2008, March). Security and privacy system architecture for an e-hospital environment. In *Proceedings of the 7th symposium on Identity and trust on the Internet* (pp. 122-130). ACM.

[122] Garzotto, F., Matera, M., & Paolini, P. (1998, May). Model-based heuristic evaluation of hypermedia usability. In *Proceedings of the working conference on Advanced visual interfaces* (pp. 135-145). ACM.

[123] Gay, V., & Leijdekkers, P. (2007). A health monitoring system using smart phones and wearable sensors'. *International Journal of ARM*, *8*(2), 29-35.

[124] Ghosh, K., Parikh, T. S., & Chavan, A. L. (2003, April). Design considerations for a financial management system for rural, semi-literate users. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems* (pp. 824-825). ACM.

[125] Gitau, S. DESIGNING UMMELI. A case for Mediated Design, a participatory approach to designing interactive systems for semi-literate users. PhD thsis, University of Cape Town, South Africa, December 2012.

[126] Goldman D. Android passes Blackberry as no 1 on smartphones. CNNMoney 2011. [Accessed: 15\03\2011], from http://money.cnn.com/2011/03/07/technology/android.

[127] Goldreich, O. (2004). *Foundations of Cryptography: Volume 2, Basic Applications* (Vol. 2). Cambridge university press.

[128] Google Android (2010). Security and permissions. [Accessed: 28/02/2011], from http://developer.android.com/intl/de/guide/topics/security/security.html.

[129] Google support. [Accessed: 14/09/2011], from http://www.google.com/support/health

[130] Gould, J. D., & Lewis, C. (1985). Designing for usability: key principles and what designers think. *Communications of the ACM*, *28*(3), 300-311.

[131] Greenbaum, J. (1993). A Design of One's own: Towards Participatory Design in the United States. In: Schuler, D. and Namioka, A. (eds.) Participatory Design Principles and Practices., pp. 27-37. Lawrence Erlbaum Associated, Inc, New Jersey.

[132] Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., & Russell, J. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *BMJ: British Medical Journal*, *341*.

[133] Greenhalgh, T., Potts, H. W., Wong, G., Bark, P., & Swinglehurst, D. (2009). Tensions and Paradoxes in Electronic Patient Record Research: A Systematic Literature Review Using the Meta-narrative Method. *Milbank Quarterly*, *87*(4), 729-788.

[134] Grimes, A., Kantroo, V., & Grinter, R. E. (2010, September). Let's play!: mobile health games for adults. In *Proceedings of the 12th ACM international conference on Ubiquitous computing* (pp. 241-250). ACM.

[135] Grimson, J. (2001a). Delivering the Electronic Healthcare Record for the 21st Century, *International Journal of Medical Informatics*, vol. 64, pp. 111-127.

[136] Grimson, J., Stephens, G., Jung, B., Grimson, W., Berry, D., & Pardon, S. (2001). Sharing health-care records over the Internet. *Internet Computing, IEEE*, *5*(3), 49-58.

[137] Guillemette, R. A. (1995). The evaluation of usability in interactive information systems. *Human factors in information systems: Emerging theoretical bases*, 207-221.

[138] Guillou, L. C., & Quisquater, J. J. (1990, February). A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In *Proceedings on Advances in cryptology* (pp. 216-231). Springer-Verlag New York, Inc..

[139] Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of Medical Internet Research*, *7*(1).

[140] Gustafson, D. H., Robinson, T. N., Ansley, D., Adler, L., & Flatley Brennan, P. (1999). Consumers and evaluation of interactive health communication applications. *American journal of preventive medicine*, *16*(1), 23-29.

[141] Haklay, M., & Tobón, C. (2003). Usability evaluation and PPGIS: towards a user-centred design approach. *International Journal of Geographical Information Science*, *17*(6), 577-592.

[142] Halamka, J. D., Mandl, K. D., & Tang, P. C. (2008). Early experiences with personal health records. *Journal of the American Medical Informatics Association*, *15*(1), 1-7.

[143] Han, D., Park, S., & Lee, M. (2008). THE-MUSS: Mobile u-health service system. In Biomedical Engineering Systems and Technologies, *International Joint Conference, BIOSTEC 2008, Revised Selected Papers,* volume 25 of Communications in Computer and Information Science, pages 377-389. Springer.

[144] Harper, R., Rodden, T., Rogers, Y., and Sellen, A. (2008). Being Human: Human Computer Interaction in the Year 2020. Cambridge, England: Microsoft Research Ltd.

[145] Harrington, A., & Jensen, C. (2003, June). Cryptographic access control in a distributed file system. In *Proceedings of the eighth ACM symposium on Access control models and technologies* (pp. 158-165). ACM.

[146] Harrison, J. P., & Lee, A. (2006). The role of e-health in the changing health care environment. *Nursing Economics*, *24*(6), 283.

[147] Hartung, C., Lerer, A., Anokwa, Y., Tseng, C., Brunette, W., and Borriello, G. (2010, December). Open data kit: Tools to build information services for developing regions. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development* (p. 18). ACM.

[148] Hassol, A., Walker, J. M., Kidder, D., Rokita, K., Young, D., Pierdon, S., ... & Ortiz, E. (2004). Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *Journal of the American Medical Informatics Association*, *11*(6), 505-513.

[149] Haux, R. (2006). Health information systems–past, present, future. *International journal of medical informatics*, *75*(3), 268-281.

[150] Health Level Seven Inc. HL7 Standards, [Accessed 12/01/2011] from www.hl7.org.

[151] HealthVault. Web application directory. [Accessed: 14/09/2011], from http://www.healthvault.com/personal/websites.html?type=application.

[152] Heeks, R. (2002). i-development not e-development: Special issue on ICTs and development. *Journal of International Development*, *14*(1), 1-11.

[153] Heeks, R. (2008). ICT4D 2.0: The Next Phase of Applying ICT for International Development. *IEEE Computer.*, *41*(6), 26–33.

[154] Helander, M. G., Landauer, T. K., & Prabhu, P. V. (Eds.). (1997). *Handbook of human-computer interaction*. Access Online via Elsevier.

[155] Hellström, J., & Tröften, P. E. (2010). *The innovative use of mobile applications in East Africa*. Swedish international development cooperation agency (Sida).

[156] HHS. Security standards - final rule 2003. [Accessed 16/05/2013], from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[157] Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure Internet banking authentication. *Security & Privacy, IEEE*, *4*(2), 21-29.

[158] HIMSS: Transforming Healthcare through IT. [Accessed: 06/08/2012], from http://www.himss.org/asp/topics_ehr.asp.

[159] HIPAA 2010. HIPAA website. [Accessed on 17 May 2013], Online at http://www.hhs.gov/ocr/privacy/.

[160] HL7 Standards. [Accessed 15/05/2013] from http://www.hl7.org/documentcenter/public_temp_970C498C-1C23-BA17-0C16CF1A10F38C87/HL7/HL7_AnnualReport_web_2009.pdf.

[161] Ho, M. R., Owusu, E. K., & Aoki, P. M. (2009, April). Claim Mobile: Engaging conflicting stakeholder requirements in healthcare in Uganda. In *Information and*

Communication Technologies and Development (ICTD), 2009 International Conference on (pp. 35-45). IEEE.

[162] Hogberg, U. (2005). The World Health Report 2005: Make every mother and child count – including Africans. *Scand J Public Health.* 33: 409–411.

[163] Holtzblatt, K., Wendell, J. B., & Wood, S. (2005). Rapid contextual design: Guide to Key Techniques for User-Centered Design, Morgan Kaufmann.

[164] Housley, R & Polk, T. (2001). Planning for PKI: best practices guide for deploying public key infrastructure. John Wiley & Sons, Inc.

[165] Housley, R., Polk, W., Ford, W., & Solo, D. (2002). Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. [Accessed: 04/10/2013], from http://www.hjp.at/doc/rfc/rfc3280.html.

[166] Hoxmeier, J. A., & DiCesare, C. (2000, August). System response time and user satisfaction: An experimental study of browser-based applications. In *Proceedings of the Association of Information Systems Americas Conference* (pp. 140-145).

[167] Hsieh, G., & Chen, R. J. (2012, December). Design for a secure interoperable cloud-based Personal Health Record service. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on* (pp. 472-479). IEEE.

[168] Hsu, J., Huang, J., Kinsman, J., Fireman, B., Miller, R., Selby, J., & Ortiz, E. (2005). Use of e-Health services between 1999 and 2002: a growing digital divide. *Journal of the American Medical Informatics Association*, *12*(2), 164-171.

[169] Hupperich, T., Löhr, H., Sadeghi, A. R., & Winandy, M. (2012, January). Flexible patient-controlled security for electronic health records. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium* (pp. 727-732). ACM.

[170] Hurtado, M. P., Swift, E. K., & Corrigan, J. M. (Eds.). (2001). *Envisioning the national health care quality report*. National Academies Press.

[171] Institute of Medicine (IOM). Committee on Quality of Health Care in America. (2001). *Crossing the quality chasm: A new health system for the 21st century*. National Academies Press.

[172] INTERFACEWARE. Open Systems vs Closed Systems. [Accessed 15/05/2013], from http://www.interfaceware.com/open_systems_vs__closed_systems.html.

[173] International Telecommunication Union 2013. Facts and figure. Accessed [March 12, 2013], from http://www.itu.int/ITU-D/ict/facts/material/ICTFactsFigures2013.pdf

[174] ISO DIS 9241-210:2008. Ergonomics of human system interaction -Part 210: Human-centred design for interactive systems (formerly known as 13407). International Standardization Organization (ISO). Switzerland.

[175] ISO FDIS 9241-210: 2009. Human-centred design process for interactive systems. International Standardization Organization (ISO).

[176] ISO: ISO 9241-11:1998 - Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) - Part 11: Guidance on Usability, 1998.

[177] iTrust: Role-Based Healthcare. [Accessed: 13/07/2011], from http://agile.csc.ncsu.edu/iTrust/wiki/doku.php?id=start.

[178] Jacko, J. A & Sears, A. (Eds.). (2003). H*uman-computer interaction* Mahwah: Lawrence Erlbaum & Associates, 2003.

[179] Jacucci, E., Shaw, V., & Braa, J. (2006). Standardization of health information systems in South Africa: The challenge of local sustainability. *Information Technology for Development*, *12*(3), 225-239.

[180] Jeffrey, R. (1994). Handbook of usability testing: How to plan, design and conduct effective tests. John Wiley & Sons, Inc; New York

[181] Jones, M. and Marsden, G. 2006. Mobile Interaction Design. John Wiley & Sons, Chichester, UK.

[182] Joshi, J. B., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM*, *44*(2), 38-44.

[183] Joye, M., & Neven, G. (Eds.). (2009). *Identity-based cryptography* (Vol. 2). IOS Press.

[184] Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, *15*(6), 729-736.

[185] Kagoda, A. M. (2012). Access to Quality Primary Education in Rural Societies of Uganda. *UNCIEF Publication*.

[186] Kaliski, B. (2000). PKCS# 5: Password-based cryptography specification version 2.0. [Accessed: 02/03/2012], from http://tools.ietf.org/html/rfc2898.

[187] Kalogriopoulos, N. A., Baran, J., Nimunkar, A. J., & Webster, J. G. (2009, September). Electronic medical record systems for developing countries: review. In *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE* (pp. 1730-1733). IEEE.

[188] Kamadjeu, R. M., Tapang, E. M., & Moluh, R. N. (2005). Designing and implementing an electronic health record system in primary care practice in sub-Saharan Africa: a case study from Cameroon. *Informatics in primary care*, *13*(3), 179-186.

[189] Kantanka, N. S. (2007). Personal health record as a backbone for primary healthcare in developing countries (Doctoral dissertation, Norwegian University of Science and Technology).

[190] Kao, Y. W., Luo, G. H., Lin, H. T., Huang, Y. K., & Yuan, S. M. (2011, October). Physical access control based on QR code. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on* (pp. 285-288). IEEE.

[191] Kaplan, W. A. (2006). Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries. *Global Health*, *2*(9).

[192] Karat, C., Brodie, C., & Karat, J. (2005). Usability design and evaluation for privacy and security solutions. In *Security and Usability: Designing Secure Systems that People Can Use*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly Media, Chapter 4, 47–74.

[193] Kawahara, Y., Takagi, T., & Okamoto, E. (2006, November). Efficient implementation of tate pairing on a mobile phone using java. In *Computational Intelligence and Security, 2006 International Conference on* (Vol. 2, pp. 1247-1252). IEEE.

[194] Kayem, A. V. D. M. *Adaptive Cryptographic Access Control for Dynamic Data Sharing Environments*. PhD thesis, Queen's University, Kingston, Ontario, Canada, October 2008.

[195] Kensing, F., & Blomberg, J. (1998). Participatory design: Issues and concerns. *Computer Supported Cooperative Work (CSCW)*, *7*(3-4), 167-185.

[196] Kenteris, M., Gavalas, D., & Economou, D. (2009). An innovative mobile electronic tourist guide application. *Personal and ubiquitous computing*, *13*(2), 103-118.

[197] Keselman, A., Slaughter, L., Arnott-Smith, C., Kim, H., Divita, G., Browne, A., ... & Zeng-Treitler, Q. (2007). Towards consumer-friendly PHRs: patients' experience with reviewing their health records. In *AMIA Annual Symposium Proceedings* (Vol. 2007, p. 399). American Medical Informatics Association.

[198] Kickbusch, I. S. (2001). Health literacy: addressing the health and education divide. *Health promotion international*, *16*(3), 289-297.

[199] Kihidis, A., Chalkias, K., & Stephanides, G. (2010, September). Practical Implementation of Identity Based Encryption for Secure E-mail Communication. In *Informatics (PCI), 2010 14th Panhellenic Conference on* (pp. 101-106). IEEE.

[200] Kim, M. I., & Johnson, K. B. (2002). Personal health records evaluation of functionality and utility. *Journal of the American Medical Informatics Association*, *9*(2), 171-180.

[201] Kind, T., & Silber, T. (2004). Ethical issues in pediatric e-health. Clinical Pediatrics, 3(7), 593-599.

[202] Kjeldskov, J., & Stage, J. (2004). New techniques for usability evaluation of mobile systems. *International Journal of Human-Computer Studies*, *60*(5), 599-620.

[203] Kleine, D., & Unwin, T. (2009). Technological Revolution, Evolution and New Dependencies: what's new about ict4d?. *Third World Quarterly*, *30*(5), 1045-1067.

[204] Kujala, S., Kauppinen, M., Nakari, P., & Rekola, S. (2003). Field studies in practice: Making it happen. In *Proceedings of INTERACT 2003* (pp. 359-366).

[205] Kulynych, J., & Korn, D. (2003). The New HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule Help or Hindrance for Clinical Research?. *Circulation*, *108*(8), 912-914.

[206] Kupchunas, W. R. (2007). Personal health record: new opportunity for patient education. *Orthopaedic Nursing*, *26*(3), 185-191.

[207] Kwankam, S. Y. (2004). What e-Health can offer. *Bulletin of the World Health Organization*, *82*(10), 800-802.

[208] Kyla, Y. (2013). Mobile phones unleash farmers in Uganda. [Accessed: 18/10/2013], from http://www.csmonitor.com/World/Making-a-difference/Change-Agent/2013/0509/Mobile-phones-unleash-farmers-in-Uganda

[209] Lafky, D. B., & Horan, T. A. (2008, January). Prospective personal health record use among different user groups: results of a multi-wave study. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 233-233). IEEE.

[210] Laukkanen, T., & Lauronen, J. (2005). Consumer value creation in mobile banking services. *International Journal of Mobile Communications*, *3*(4), 325-338.

[211] Lawton, G. (2002). Moving Java into mobile phones. *Computer*, *35*(6), 17-20.

[212] Lee, K. B., & Grice, R. A. (2004). Developing a new usability testing method for mobile devices. In *Professional Communication Conference, 2004. IPCC 2004. Proceedings. International* (pp. 115-127). IEEE.

[213] Lee, Y., Lee, J., & Song, J. (2007). Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. *Computer Communications*, *30*(4), 893-903.

[214] Leonard, K. J. (2004). The role of patients in designing health information systems: the case of applying simulation techniques to design an electronic patient record (EPR) interface. *Health Care Management Science*, *7*(4), 275-284.

[215] Lewis, C., & Rieman, J. (1994). Task-centred user interface design. [Accessed: 09 August 2013], Available via http://web.cs.dal.ca/~jamie/TCUID/tcuid.pdf.

[216] Lewis, J. R. (1992, October). Psychometric evaluation of the post-study system usability questionnaire: The PSSUQ. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 36, No. 16, pp. 1259-1260). SAGE Publications.

[217] Lewis, J. R. (1995). IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use. *International Journal of Human‐Computer Interaction*, *7*(1), 57-78.

[218] Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *Security and Privacy in Communication Networks* (pp. 89-106). Springer Berlin Heidelberg.

[219] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption.

[220] Liff, S., Shepherd, A., Wajcman, J., Rice, R., & Hargittai, E. (2004). An evolving gender digital divide?. *OII Internet Issue Brief*, (2).

[221] Lightner, N. J., Bose, I., & Salvendy, G. (1996). What is wrong with the World-Wide Web?: a diagnosis of some problems and prescription of some remedies. *Ergonomics*, *39*(8), 995-1004.

[222] Lindgaard, G. (1994). *Usability testing and system evaluation: A guide for designing useful computer systems* (pp. 221-246). London: Chapman & Hall.

[223] Lober, W. B., Zierler, B., Herbaugh, A., Shinstrom, S. E., Stolyar, A., Kim, E. H., & Kim, Y. (2006). Barriers to the use of a personal health record by an elderly population. In *AMIA Annual Symposium Proceedings* (Vol. 2006, p. 514). American Medical Informatics Association.

[224] Löhr, H., Sadeghi, A. R., & Winandy, M. (2010, November). Securing the e-health cloud. In *Proceedings of the 1st ACM International Health Informatics Symposium* (pp. 220-229). ACM.

[225] Luk, R., Zaharia, M., Ho, M., Levine, B., & Aoki, P. M. (2009, April). ICTD for healthcare in Ghana: two parallel case studies. In *Information and Communication*

Technologies and Development (ICTD), 2009 International Conference on (pp. 118-128). IEEE.

[226] Lysyanskaya, A., Rivest, R. L., Sahai, A., & Wolf, S. (2000, January). Pseudonym systems. In *Selected Areas in Cryptography* (pp. 184-199). Springer Berlin Heidelberg.

[227] Mack, R. L., & Nielsen, J. (Eds.). (1994). *Usability inspection methods*. Wiley & Sons.

[228] Madrigal, D. & McClain, B. (2010). Do's and Don'ts of Usability Testing. [Accessed: 18/09/2013] from http://www.uxmatters.com/mt/archives/2010/03/dos-and-donts-of-usability-testing.php.

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

[230] Mandl, K. D., & Kohane, I. S. (1999). Healthconnect: clinical grade patient-physician communication. In *Proceedings of the AMIA Symposium* (p. 849). American Medical Informatics Association.

[231] Mandl, K. D., Mandel, J. C., Murphy, S. N., Bernstam, E. V., Ramoni, R. L., Kreda, D. A., ... & Kohane, I. S. (2012). The SMART Platform: early experience enabling substitutable applications for electronic health records. *Journal of the American Medical Informatics Association*, *19*(4), 597-603.

[232] Mandl, K. D., Simons, W. W., Crawford, W. C., & Abbett, J. M. (2007). Indivo: a personally controlled health record for health information exchange and communication. *BMC medical informatics and decision making*, *7*(1), 25.

[233] Mandl, K.D.; Szolovits P. & Kohane I.S. (2001). Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private. *BMJ* 322:283-287.

[234] Mao, J. Y., Vredenburg, K., Smith, P. W., & Carey, T. (2005). The state of user-centered design practice. *Communications of the ACM*, *48*(3), 105-109.

[235] Marczak, M., & Sewell, M. (2006). Using focus groups for evaluation. *Cybernet Evaluation. Tuscon, AZ: The University of Arizona*.

[236] Mars, M. & Seebregts, C. (2008). Country case study for e-health: South Africa. [Accessed 11/08/2012], from http://archive.k4health.org/system/files/County%20Case%20Study%20for%20eHealth%20South%20Africa.pdf.

[237] Marsden, G., Maunder, A., & Parker, M. (2008). People are people, but technology is not technology. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *366*(1881), 3795-3804.

[238] Masys, D., Baker, D., Butros, A., & Cowles, K. E. (2002). Giving Patients Access to Their Medical Records via the Internet The PCASSO Experience. *Journal of the American Medical Informatics Association*, *9*(2), 181-191.

[239] Mayhew, D. J. (1991). *Principles and guidelines in software user interface design*. Prentice-Hall, Inc.

[240] Mayhew, D. J. (1999). The usability engineering lifecycle. San Francisco, CA. Morgan Kaufmann Publishers, Inc.

[241] McGinn, C. A., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L., ... & Gagnon, M. P. (2011). Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: a systematic review. *BMC medicine*, *9*(1), 46.

[242] McNamara, K. S. (2003). Information and Communication Technologies, Poverty and Development: Learning from Experience. A Background Paper for the *InfDev Annual Symposium, 9–10 December 2003, Geneva, Switzerland.*

[243] Mechael, P. N. (2009). The case for mHealth in developing countries. *innovations*, *4*(1), 103-118.

[244] Medhi, I., Sagar, A., & Toyama, K. (2006, May). Text-free user interfaces for illiterate and semi-literate users. In *Information and Communication Technologies and Development, 2006. ICTD'06. International Conference on* (pp. 72-82). IEEE.

[245] MediCompass. [Accessed: 13/08/2011], from https://www.medicompass.com/mcweb/default.aspx.

[246] Meidani, Z., Sadoughi, F., Maleki, M. R., Tofighi, S., & Marani, A. B. (2012). Organization’s quality maturity as a vehicle for EHR success. *Journal of medical systems*, *36*(3), 1229-1234.

[247] Meingast, M., Roosta, T., & Sastry, S. (2006, August). Security and privacy issues with health care information technology. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE* (pp. 5453-5458). IEEE.

[248] Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, *47*(7), 25-28.

[249] Millen, D. R. (2000, August). Rapid ethnography: time deepening strategies for HCI field research. In *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques* (pp. 280-286). ACM.

[250] Miller, V. S. (1986, January). Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO'85 Proceedings* (pp. 417-426). Springer Berlin Heidelberg.

[251] Mitamura, Y., Yamamoto, A., Hayashi, H., Namioka, T., Tsuduki, Y., Shimono, T., ... & Yoshida, A. (2005, May). A peer-to-peer-based medical information sharing system. In *Electrical and Computer Engineering, 2005. Canadian Conference on* (pp. 378-381). IEEE.

[252] Mohan, A., Bauer, D., Blough, D. M., Ahamad, M., Bamba, B., Krishnan, R., ... & Palanisamy, B. (2009). A patient-centric, attribute-based, source-verifiable framework for health record sharing. CERCS Tech Report GIT-CERCS-09-11, Georgia Tech, 2009.

[253] Montgomery, M. R., & Hewett, P. C. (2005). Urban poverty and health in developing countries: household and neighborhood effects. *Demography*, *42*(3), 397-425.

[254] Moore, J. (2009). The feds and PHR privacy. Government Health IT. [Accessed: 13/09/2012], from http://www.govhealthit.com/Articles/2009/01/26/The-feds-and-PHR-privacy.aspx

[255] Morrison, M. J., & Boumphrey, F. D., and Brownel. (2000) XML Unleashed, Sams Publishing.

[256] Mthoko, H. L., & Pade-Khene, C. (2013). Towards a theoretical framework on ethical practice in ICT4D programmes. *Information Development*, *29*(1), 36-53.

[257] Mugwanya, R. (2013). Software support for creating mobile content for education. (Doctoral dissertation, DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF SCIENCE, UNIVERSITY OF CAPE TOWN).

[258] Muller, M. J., & Kuhn, S. (1993). Participatory design. *Communications of the ACM*, *36*(6), 24-28.

[259] Müller, M. L., Ückert, F., Bürkle, T., & Prokosch, H. U. (2005). Cross-institutional data exchange using the clinical document architecture (CDA). *International journal of medical informatics*, *74*(2), 245-256.

[260] Myhealthfolders. [Accessed: 13/08/2011], from https://myhealthfolders.com/

[261] Mymedicalrecords.com. [11/08/2011], from https://www.mymedicalrecords.com/login.jsp.

[262] Nah, F. F. H. (2004). A study on tolerable waiting time: how long are web users willing to wait?. *Behaviour & Information Technology*, *23*(3), 153-163.

[263] Naor, M., & Yung, M. (1990, April). Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing* (pp. 427-437). ACM.

[264] Narayan, S., Gagné, M., & Safavi-Naini, R. (2010, October). Privacy preserving EHR system using attribute-based infrastructure. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* (pp. 47-52). ACM.

[265] National Committee on Vital and Health Statistics (NCVHS), Personal Health Records and Personal Health Record Systems (Washington, DC: U.S. Department of Health and Human Services), p. 15; [Accessed 23/05/2013], from http://www.ncvhs.hhs.gov/0602nhiirpt.pdf.

[266] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-4, March 2012, [Accessed: 08/11/2013], from http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

[267] Nauman, M., Khan, S., & Zhang, X. (2010, April). Apex: extending android permission model and enforcement with user-defined runtime constraints. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (pp. 328-332). ACM.

[268] NHS. (2009). UK National Health Service. Connecting for Health. [Accessed 17th November 2012], Online at http://www.connectingforhealth.nhs.uk.

[269] Nielsen, J. (1990). Traditional dialogue design applied to modern user interfaces. *Communications of the ACM*, *33*(10), 109-118.

[270] Nielsen, J. (1993). Usability Engineering. Morgan Kaufmann. Academic Press; New York.

[271] Nielsen, J. (1994a). Heuristic evaluation. *Usability inspection methods*, *17*, 25-62.

[272] Nielsen, J. (1994b). Estimating the number of subjects needed for a thinking aloud test. *International journal of human-computer studies*, *41*(3), 385-397.

[273] Nielsen, J. (1994d). Guerrilla HCI: Using discount usability engineering to penetrate the intimidation barrier, Cost-justifying usability, pp. 245–272.

[274] Nielsen, J. (1997). The need for speed. *Alertbox (web page: http://www. useit. com/alertbox/9703a. html)*.

[275] Nielsen, J. (1997b). The use and misuse of focus groups. *Software, IEEE*, *14*(1), 94-95.

[276] Nielsen, J. (1999). User interface directions for the web. *Communications of the ACM*, *42*(1), 65-72.

[277] Nielsen, J. (2000). Designing Web Usability: The Practice of Simplicity (Indianapolis: New Riders).

[278] Nielsen, J. (2002). Field studies done right: Fast and observational. *Jakob Nielsen's Alertbox, January 20*.

[279] Nielsen, J., & Molich, R. (1990, March). Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 249-256). ACM.

[280] NIST. Test procedure for 170.302 (o) Access control. [04/08/2012], from http://healthcare.nist.gov/docs/170.302.o_AccessControl_v1.1.pdf.

[281] NZPA. (1993). Privacy act 1993. New Zealand legislature, Public Act 1993 No. 28. [Accessed 17th May 2013], from http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html#whole.

[282] O'Donnell, P. J., Scobie, G.E.W., and Baxter, I. (1991). *The use of focus groups as an evaluation technique in HCI.* In: Diaper, D. and Hammond, H. (eds.) People and Computers VI: Proceedings of the HCI '91 Conference. Cambridge University Press, pp. 211-224. ISBN 9780521416948

[283] Obrist, M., Roto, V., & Väänänen-Vainio-Mattila, K. (2009, April). User experience evaluation: do you know which method to use?. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems* (pp. 2763-2766). ACM.

[284] Ojo, T. (2007). ICTs for development in the sub-Saharan African region: historical, economical and political context. Paper presented at *The Annual Meeting of the International Communication Association, Sheraton, New York*.

[285] Olla, P., & Tan, J. (2006). The M-health reference model: An organising framework for conceptualizing mobile health systems. *International journal of healthcare information systems and informatics* 1: 1 – 19.

[286] Omary, Z., Lupiana, D., Mtenzi, F., & Wu, B. (2009, July). Challenges to E-healthcare adoption in developing countries: A case study of Tanzania. In *Networked Digital Technologies, 2009. NDT'09. First International Conference on* (pp. 201-209). IEEE.

[287] Open EMR. [12/07/2011], from http: //www.oemr.org/

[288] Oppliger, R. (1996). *Authentication System for Secure Networks*, Artech House INC, Boston, MA.

[289] Oppliger, R., Hauser, R., & Basin, D. (2008). SSL/TLS session-aware user authentication. *Computer*, *41*(3), 59-65.

[290] Palen, L., & Salzman, M. (2002). Beyond the handset: designing for wireless communications usability. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *9*(2), 125-151.

[291] Parameswaran, T., Vanitha, S., & Arvind, K. S. (2013). An Efficient Sharing of Personal Health Records Using DABE in Secure Cloud Environment. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(3), pp-0925.

[292] Parikh, T. S., & Lazowska, E. D. (2006, May). Designing an architecture for delivering mobile information services to the rural developing world. In *Proceedings of the 15th international conference on World Wide Web* (pp. 791-800). ACM.

[293] Parikh, T., S. (2007). Designing an architecture for Delivering Mobile Information Services to the Rural Developing World. Doctor of Philosophy thesis, University of Washington, USA. [Accessed: 07-06-2012], from http://people.ischool.berkeley.edu/~parikh/papers/parikh-thesis.pdf.

[294] PBC library. The Pairing-Based Cryptography Library. [Online] Available: http://crypto.stanford.edu/ibe/ [Accessed: 06-08-2012].

[295] Peters, T. (2001). Spanning the Digital Divide–understanding and tackling the issues. *Bridges. org, Washington/Durbanville*, 152.

[296] Petrogiannis, Y. (1999). Healthcare: Secure healthcare documents with electronic approval, Inform, vol. 13, Iss.8, pp. 12.

[297] Pitkow, J. E., & Kehoe, C. M. (1996). Emerging trends in the WWW user population. *Communications of the ACM*, *39*(6), 106-108.

[298] Pitula, K., Dysart-Gale, D., & Radhakrishnan, T. (2010). Expanding Theories of HCI: a case study in requirements engineering for ICT4D. *Information Technologies & International Development*, *6*(1), pp-78.

[299] Pope, C., Ziebland, S., & Mays, N. (2000). Qualitative research in health care: Analysing qualitative data. *BMJ: British Medical Journal*, *320*(7227), 114.

[300] Preece, J., Rogers, Y., & Sharp, H. (2002). Interaction design: Beyond human-computer interaction. New York, NY: John Wiley & Sons.

[301] Preece, J., Rogers, Y., Sharp, H., Benyon, D., & Holland, T. (1994). S. Carey. *Human-Computer Interaction. Addison-Wesley, Wokingham, England*.

[302] President's Council of Advisors on Science and Technology, "Realizing the full potential of health information technology to improve healthcare for Americans: The path forward," Executive Office of the President, Tech. Rep., 2010. [Accessed: 14/05/2013], from http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

[303] Raiti, G. C. (2007). The lost sheep of ICT4D literature. *Information Technologies and International Development*, *3*(4), 1-8.

[304] Ramachandran, D., Kam, M., Chiu, J., Canny, J., & Frankel, J. F. (2007). Social dynamics of early stage co-design in developing regions. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 1087-1096). ACM.

[305] Rashid, A. T., & Elder, L. (2009). Mobile phones and development: An Analysis of IDRC-supported projects. *The Electronic Journal of Information Systems in Developing Countries*, *36*.

[306] Rassinoux, A. M., Lovis, C., Baud, R., & Geissbuhler, A. (2003). XML as standard for communicating in a document-based electronic patient record: a 3 years experiment. *International journal of medical informatics*, *70*(2), 109-115.

[307] Reed S. Who defines Usability? You do! PC Computing 1992; 5(12):220–232.

[308] Reis, C. I., Freire, C. S., Fern´andez, J & Monguet, J., M. (2011). Patient centered design: challenges and lessons learned from working with health professionals and schizophrenic patients in e-therapy contexts. *Communications in Computer and Information Science*, *vol. 221, no. 1,* pp. 1–10.

[309] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[310] Robison, J., Bai, L., Mastrogiannis, D. S., Tan, C. C., & Wu, J. (2012, October). A survey on PHR technology. In *e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on* (pp. 184-189). IEEE.

[311] Rodriguez, M. M., Casper, G., & Brennan, P. F. (2007). Patient-centred design: the potential of user-centred design in personal health records. *JOURNAL-AHIMA*, *78*(4), 44.

[312] Rogers, Y. (2004). New theoretical approaches for human-computer interaction. *Annual review of information science and technology*, *38*(1), 87-143.

[313] Rogers, Y., Connelly, K., Tedesco, L., Hazlewood, W., Kurtz, A., Hall, R. E., ... & Toscos, T. (2007). Why it's worth the hassle: The value of in-situ studies when designing UbiComp. In *UbiComp 2007: Ubiquitous Computing* (pp. 336-353). Springer Berlin Heidelberg.

[314] Rogers, Y., Sharp, H. & Preece, J (2011). Interaction Design: Beyond Human-Computer Interaction, 3rd Edition, John Wiley and Sons, Ltd, publication.

[315] Rogers, Y.; Sharp, H. & Preece, J. (2007). Interaction Design: Beyond Human-Computer Interaction (2nd edn). John Wiley & Sons

[316] Ross, S. E., Earnest, M. A., Lin, C. and Wittevrongel, L. (2002 May). Providing patient access to online medical records: A compression of physician and patient expectations. In 25th Annual Meeting, Society of General internal Medicine.

[317] Rouvinen, P. (2006). Diffusion of digital mobile telephony: Are developing countries different?. *Telecommunications Policy*, *30*(1), 46-63.

[318] Sachs, G. S. (2004). Strategies for improving treatment of bipolar disorder: integration of measurement and management. *Acta Psychiatrica Scandinavica*, *110*(s422), 7-17.

[319] Sachs, J. (2008). The end of poverty: economic possibilities for our time. *European Journal of Dental Education* 12, no. s1: 17-21.

[320] Sahlfeld, M. (2007). How does ICT work for development? A review of the challenges and opportunities. *ATDF Journal*, *4*(1), 22-36.

[321] Saleh, M., & Al Khatib, I. (2005, September). Throughput analysis of WEP security in ad hoc sensor networks. In *The Second International Conference on Innovations in Information Technology (IIT'05), Dubai*.

[322] Sanders, C., Rogers, A., Bowen, R., Bower, P., Hirani, S., Cartwright, M., ... & Newman, S. P. (2012). Exploring barriers to participation and adoption of telehealth and telecare within the Whole System Demonstrator trial: a qualitative study. *BMC health services research*, *12*(1), 220.

[323] Sax, U., Kohane, I., & Mandl, K. D. (2005). Wireless technology infrastructures for authentication of patients: PKI that rings. *Journal of the American Medical Informatics Association*, *12*(3), 263-268.

[324] Scaife, M., & Rogers, Y. (1999). Kids as informants: Telling us what we didn't know or confirming what we knew already. *The design of children's technology*, 27-50.

[325] Schuler, D., & Namioka, A. (Eds.). (1993). *Participatory design: Principles and practices*. Routledge.

[326] Schwingenschlögl, C., Eichler, S., & Müller-Rathgeber, B. (2006). Performance of PKI-based security mechanisms in mobile ad hoc networks. *AEU-International Journal of Electronics and Communications*, *60*(1), 20-24.

[327] Scriven, M. (1991) Evaluation Thesaurus (fourth edition). Sage, London

[328] Seltzer, L. (2010). Protecting Your Code Updates: How to Defend Against SSL Spoofing Attacks, 2010. [Accessed 27th May 2013], from https://www.secure128.com/documents/Code_Signing_White_Paper_Protecting_Your_Code.pdf.

[329] Selvidge, P. (2003). Examining tolerance for online delays. *Usability News*, *5*(1), 1-5. [Accessed: 23/08/2013], from http://psychology.wichita.edu/surl/usabilitynews/51/pdf/Usability%20News%2051%20-%20Selvidge.pdf.

[330] Seppälä, P., & Alamäki, H. (2003). Mobile learning in teacher training. *Journal of computer assisted learning*, *19*(3), 330-335.

[331] Shackel, B. (1991). Usability-context, framework, definition, design and evaluation. *Human factors for informatics usability*, 21-37.

[332] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53.

[333] Sharedhealth, Transforming Care. [Accessed: 1/09/2011], from http://www.sharedhealth.com/.

[334] Sharples, M., Corlett, D., & Westmancott, O. (2002). The design and implementation of a mobile learning resource. *Personal and Ubiquitous Computing*, *6*(3), 220-234.

[335] Siau, K., & Tan, X. (2005). Improving the quality of conceptual modeling using cognitive mapping techniques. *Data & Knowledge Engineering*, *55*(3), 343-365.

[336] Silber, D. (2003). The case for eHealth. European Institute of Public Administration.

[337] Sittig, D. F. (2002). Personal health records on the Internet: a snapshot of the pioneers at the end of the 20th Century. *International journal of medical informatics*, *65*(1), 1-6.

[338] SmartPHR. Smart health records for smart people. [Accessed: 30/08/2012], from http://www.thesmartphr.com/support.php.

[339] Smith, B., Austin, A., Brown, M., King, J. T., Lankford, J., Meneely, A., & Williams, L. (2010, October). Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In *Proceedings of the second annual workshop on Security and privacy in medical and home-care systems* (pp. 1-12). ACM.

[340] Snyder, C. (2003). *Paper prototyping: The fast and easy way to design and refine user interfaces*. Morgan Kaufmann.

[341] Sood, S. P., Nwabueze, S. N., Mbarika, V. W. A., Prakash, N., Chatterjee, S., Ray, P., & Mishra, S. (2008, January). Electronic medical records: a review comparing the challenges in developed and developing countries. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 248-248). IEEE.

[342] Spinuzzi, C. (2005). The methodology of participatory design, Technical Communication, vol. 52, no. 2, pp. 163–174.

[343] Ssembatya, R. (2012). An Access Control Framework for Protecting Mobile Health Records: The Case Study of Developing Countries, *In the proceedings of the 9th International Network Conference (INC 2012),* Nelson Mandela Metropolitan University, South Africa, pp. 73- 82.

[344] Standard, A. S. T. M. (2009). E2369-05e1 “Standard Specification for Continuity of Care Record (CCR)”. *West Conshohocken, PA: ASTM International.*

[345] Stewart, D. W., Shamdasani, P. N., & Rook, D. W. (2007). *Focus groups: Theory and practice* (Vol. 20). Sage.

[346] Sun, J., Zhu, X., Zhang, C., & Fang, Y. (2011, June). Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare. In *Distributed Computing Systems (ICDCS), 2011 31st International Conference on* (pp. 373-382). IEEE.

[347] Sundén, S. & Wicander, G. (2006) Information and Communication Technology Applied for Developing Countries in a Rural Context – Towards a Framework for Analyzing Factors Influencing Sustainable Use. (Karlstad University Studies 2006:69). Karlstad: Karlstad University Studies.

[348] Sunyaev, A., Chornyi, D., Mauro, C., & Kremar, H. (2010, January). Evaluation framework for personal health records: Microsoft HealthVault vs. Google Health. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1-10). IEEE.

[349] Sunyaev, A., Leimeister, J. M., & Krcmar, H. (2010). Open security issues in German healthcare telematics. *In Proceedings of the 3rd International Conference on Health Informatics*, pp. 187-194.

[350] Szolovits, P., & Kohane, I. (1994). Against simple universal health-care identifiers. *Journal of the American Medical Informatics Association*, *1*(4), 316-319.

[351] Takemura, T., Araki, K., Arita, K., Suzuki, T., Okamoto, K., Kume, N., ... & Yoshihara, H. (2012). Development of fundamental infrastructure for nationwide EHR in Japan. *Journal of medical systems*, *36*(4), 2213-2218.

[352] Tanenbaum, A. S., & Van Steen, M. (2002). *Distributed systems* (Vol. 2). Prentice Hall.

[353] Tang, D., & Lansky, D, (2005). The Missing Link: Bridging the patent provider health information gap. Health Affairs, 24 (5), 1290-1295.

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

[355] Tassie, J., Balandine, S., Szumilin, E., Andrieux-Meyer, I., Biot, M., Cavailler, P., ... & Legros, D. (2002, July). FUCHIA: a free computer program for the monitoring of HIV/AIDS medical care at the population level. In *Int Conf AIDS* (Vol. 14, p. C11029).

[356] Tessier, C. (2004). Continuity of Care Record. *ASTM E31-WG on CCR, 21st TEPR*, 16-18.

[357] Thakkar, M., & Davis, D. C. (2006). Risks, barriers, and benefits of EHR systems: a comparative study based on size of hospital. *Perspectives in Health Information Management/AHIMA, American Health Information Management Association*, *3*.

[358] The Bouncy Castle website. [Online]. Available: http://www.bouncycastle.org/ [Accessed: 06-08-2012].

[359] The health telematics working group of the high level committee on health: Final Report (2003). [Accessed 01/10/2013], from http://ec.europa.eu/health/ph_overview/Documents/hlch_health_telematics_final_report_en.pdf.

[360] The Java Pairing Based Cryptography Library (jPBC). [Online] Available: http://gas.dia.unisa.it/projects/jpbc/ [Accessed: 27-02-2012].

[361] The MIRACL crypto SDK website. [Online] Available: http://certivox.com/index.php/solutions/miracl-crypto-sdk/. [Accessed: 06-08-2012].

[362] The Personal Health Working Group: Markle Foundation; 2003.

[363] The State of Uganda Population Report 2013. Accessed: 22/05/2014, from http://popsec.org/wp-content/uploads/2013/10/SUPRE-REPORT-2013.pdf

[364] The Tolven Open Source Project. [Accessed: 15/07/2011], from www.tolven.org.

[365] Tierney, W. M., Achieng, M., Baker, E., Bell, A., Biondich, P., Braitstein, P., ... & Tanzania-Uganda OpenMRS Consortium. (2010). Experience implementing electronic health records in three East African countries. *Stud Health Technol Inform*, *160*(Pt 1), 371-375.

[366] Tiglao, N., & Alampay, E. A. (2009). Mapping ICT4D projects in the Philippines. *Philippine Journal of Public Administration*, *129*, 26-4.

[367] Tran, D. T., Zhang, X., Stolyar, A., & Lober, W. B. (2005). Patient-centred design for a personal health record system. In *AMIA Annual Symposium Proceedings* (Vol. 2005, p. 1140). American Medical Informatics Association.

[368] Tsai, C. C., Lee, G., Raab, F., Norman, G. J., Sohn, T., Griswold, W. G., & Patrick, K. (2007). Usability and feasibility of PmEB: a mobile phone application for monitoring real time caloric balance. *Mobile networks and applications*, *12*(2-3), 173-184.

[369] Turan, M. S., Barker, E., Burr, W., & Chen, L. (2010). Recommendation for password-based key derivation. *NIST special publication*, *800*, 132.

[370] Tuyikeze, T. (2005). *A model for information security management and regulatory compliance in the South African health sector.* MSc thesis. Nelson Mandela Metropolitan University. [Accessed: 01/08/2012], from http://www.nmmu.ac.za/documents/theses/Thesis_TITE.pdf. Accessed 01/08/2012.

[371] Tuyikeze, T., & Pottas, D. (2005, June). Information Security Management and Regulatory Compliance in the South African Health Sector. In *ISSA* (pp. 1-12).

[372] UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990, [Accessed 17 May 2013], from http://www.refworld.org/docid/3ddcafaac.html.

[373] UNESCO Institute for Statistics, adult and youth literacy: global trends in gender parity, September 2010. [Accessed: 02/10/2013], from http://www.unesco.org/education/ild2010/FactSheet2010_Lit_EN.pdf.

[374] United Nations. (1954). Report on international definition and measurement of standards and levels of living. New York: United Nations.

[375] United Nations. (1961). Report on International definition and measurement of levels of living: An interim guide. New York: United Nations, 1961.

[376] United Nations. (2005, January 19). Tsunami survivors give birth without basic necessities. [Accessed: 12\03\2011], from http://www.un.org/News/Press/docs/2005/iha999.doc.htm.

[377] Unwin, T. (2009). ICT4D: Information and Communication for Development. UK: Cambridge University Press.

[378] Vala, R. A. D. E. K., Sarga, L. I. B. O. R., & Benda, R. A. D. E. K. (2013, July). Security Reverse Engineering of Mobile Operating Systems: A Summary. In *Recent Advances in Cimputer science. Proceedings of the 17th International Conference on computers. Rhodes Island, Greece.*

[379] Van Someren, M. W., Barnard, Y. F., & Sandberg, J. A. (1994). *The think aloud method: A practical guide to modelling cognitive processes* (p. 26). London: Academic Press.

[380] Vermeeren, A. P., Law, E. L. C., Roto, V., Obrist, M., Hoonhout, J., & Väänänen-Vainio-Mattila, K. (2010, October). User experience evaluation methods: current state and development needs. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries* (pp. 521-530). ACM.

[381] Vines, R. D. (2002). *Wireless security essentials: defending mobile systems from data piracy*. Wiley. com.

[382] VitalChart. A secure place to manage your health. [Accessed 30/08/2012], from https://www.vitalchart.com/.

[383] Volonino, L., & Robinson, S.R. (2004) Principles and practice of information security: Protecting computers from Hackers and Lawyers, *Prentice Hall, Inc., Upper Saddle River, NJ.*

[384] Voltage security. The Identity-Based Encryption Advantage. A proven standard for protecting information, technical report, 2013. [Accessed 30th May 2013], from http://www.voltage.com/wp-content/uploads/Voltage_Technical_Brief_SecureMail_The_IBE_Advantage.pdf

[385] W3C Mobile Web Best Practices 1.0, Basic Guidelines, W3C Candidate Recommendation. [Accessed: 23/04/2013], from http://www.w3.org/TR/2006/CR-mobile-bp-20060627/#requirements.

[386] Wang, C., Liu, X., & Li, W. (2012, September). Implementing a Personal Health Record Cloud Platform Using Ciphertext-Policy Attribute-Based Encryption. In *Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on* (pp. 8-14). IEEE.

[387] Weitzman, E. R., Kaci, L., & Mandl, K. D. (2009). Acceptability of a personally controlled health record in a community-based setting: implications for policy and design. *Journal of medical Internet research*, *11*(2).

[388] Wicander, G. (2011). *Mobile Supported E-Government Systems: Analysis of the Education Management Information System (EMIS) in Tanzania* (Doctoral dissertation, Karlstad University).

[389] Win, K. T., Susilo, W., & Mu, Y. (2006). Personal health record systems and their security protection. *Journal of Medical Systems*, *30*(4), 309-315.

[390] Wixon, D. R., Ramey, J., Holtzblatt, K., Beyer, H., Hackos, J., Rosenbaum, S., ... & Laakso, K. P. (2002, April). Usability in practice: field methods evolution and revolution. In *CHI'02 Extended Abstracts on Human factors in computing systems* (pp. 880-884). ACM.

[391] Wolff, A. C., Mludek, V., van der Haak, M., Bork, W., Bulzebruck, H., Drings, P., ... & Haux, R. (2001). Using the eXtensible Markup Language (XML) in a regional electronic patient record for patients with malignant diseases. *Studies in health technology and informatics*, (1), 698-702.

[392] World Health Organisation (WHO) 2005. Knowledge management strategy. Geneva. [Accessed:27/09/2012], from http://www.who.int/kms/about/strategy/kms_strategy.pdf

[393] World Wide Web Consortium (W3C). Extensible Markup Language (XML) 1.0, 3rd ed. November, 2008. [Accessed 16/05/2013] from http://www.w3.org/TR/REC-xml.

[394] WorldMedcard. [Accessed: 28/08/2011], from http://www.worldmedcard.com/.

[395] Yogeswaran, P., & Wright, G. (2010). EHR Implementation in South Africa: How do we get it right? *Studies in health technology and informatics*, *160*(Pt 1), 396.

[396] Young, S. T., & Chang, J. S. (1997). Implementation of a patient-centred and physician-oriented healthcare information system. *Informatics for Health and Social Care*, *22*(3), 207-214.

[397] Zhang, D., & Adipat, B. (2005). Challenges, methodologies, and issues in the usability testing of mobile applications. *International Journal of Human-Computer Interaction*, *18*(3), 293-308.

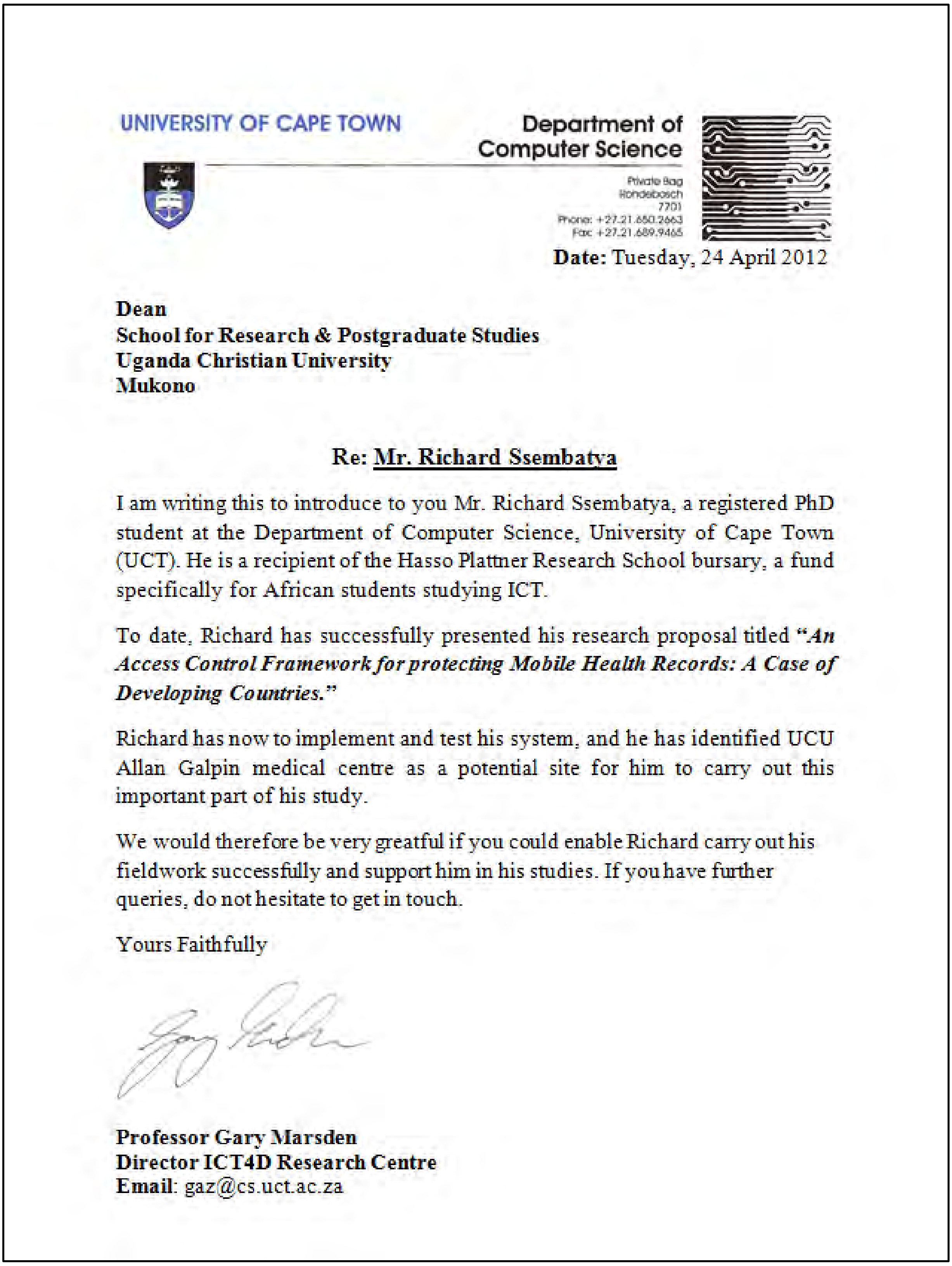
[398] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 268-275). IEEE.

[399] Zheng, K., Padman, R., Johnson, M. P., & Diamond, H. S. (2005). Understanding technology adoption in clinical care: clinician adoption behavior of a point-of-care reminder system. *International journal of medical informatics*, *74*(7), 535-543.

[400] Zheng, Y. (2011). *Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption* (Doctoral dissertation, WORCESTER POLYTECHNIC INSTITUTE).

[401] Zona research report 1999, The Need for Speed, July 1999.

APPENDIX 4: RESEARCH SUPPORT AND ETHICAL CLEARANCE LETTERS



UNIVERSITY OF CAPE TOWN

Department of
Computer Science

Private Bag
Rondebosch
7701
Phone: +27.21.650.2663
Fax: +27.21.689.9465

Date: Tuesday, 24 April 2012

Dean
School for Research & Postgraduate Studies
Uganda Christian University
Mukono

Re: Mr. Richard Ssembatya

I am writing this to introduce to you Mr. Richard Ssembatya, a registered PhD student at the Department of Computer Science, University of Cape Town (UCT). He is a recipient of the Hasso Plattner Research School bursary, a fund specifically for African students studying ICT.

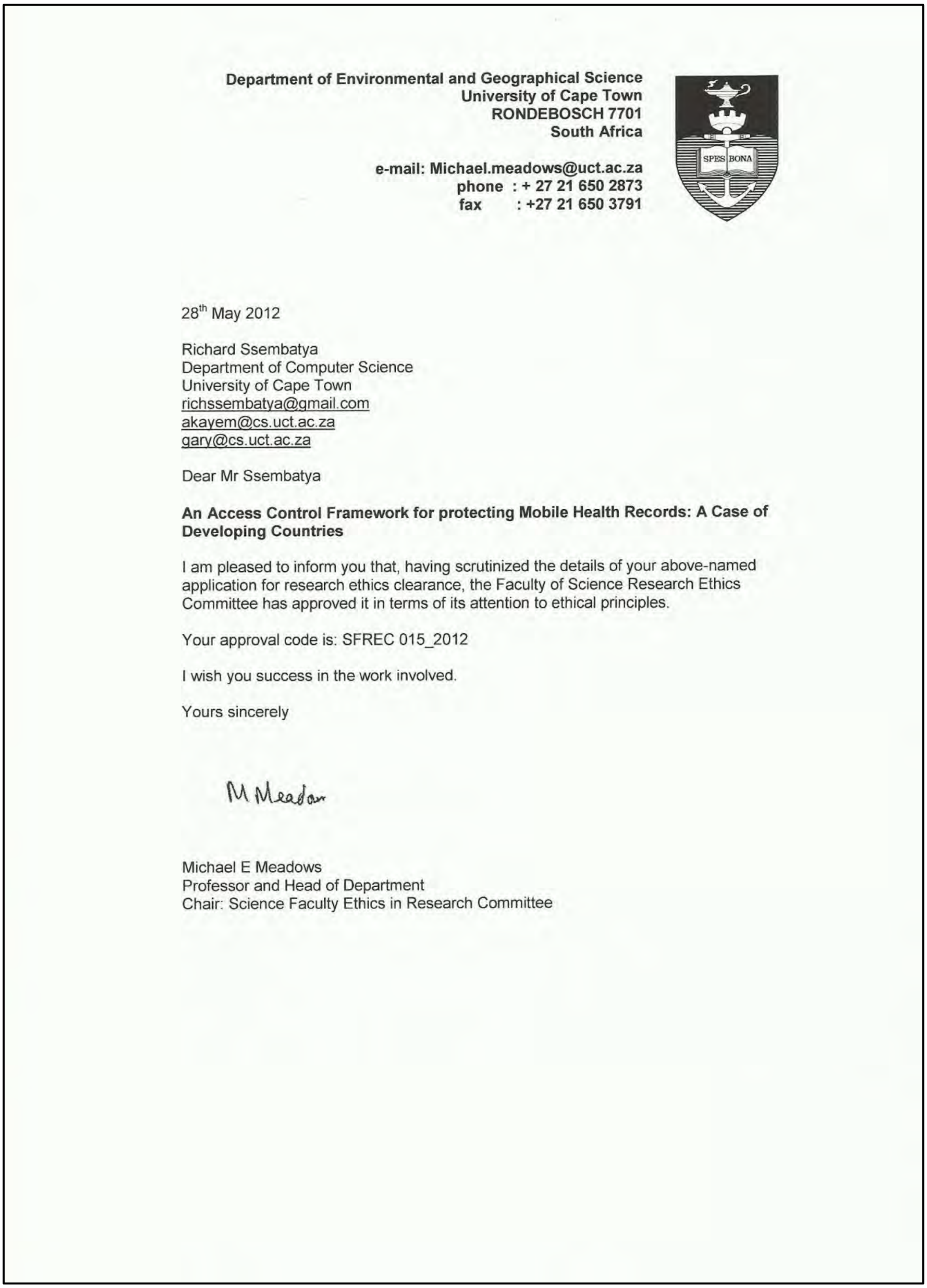
To date, Richard has successfully presented his research proposal titled ***"An Access Control Framework for protecting Mobile Health Records: A Case of Developing Countries."***

Richard has now to implement and test his system, and he has identified UCU Allan Galpin medical centre as a potential site for him to carry out this important part of his study.

We would therefore be very greatful if you could enable Richard carry out his fieldwork successfully and support him in his studies. If you have further queries, do not hesitate to get in touch.

Yours Faithfully

Professor Gary Marsden
Director ICT4D Research Centre
Email: gaz@cs.uct.ac.za



Department of Environmental and Geographical Science
University of Cape Town
RONDEBOSCH 7701
South Africa

e-mail: Michael.meadows@uct.ac.za
phone : + 27 21 650 2873
fax : +27 21 650 3791

28th May 2012

Richard Ssembatya
Department of Computer Science
University of Cape Town
richssembatya@gmail.com
akayem@cs.uct.ac.za
gary@cs.uct.ac.za

Dear Mr Ssembatya

An Access Control Framework for protecting Mobile Health Records: A Case of Developing Countries

I am pleased to inform you that, having scrutinized the details of your above-named application for research ethics clearance, the Faculty of Science Research Ethics Committee has approved it in terms of its attention to ethical principles.

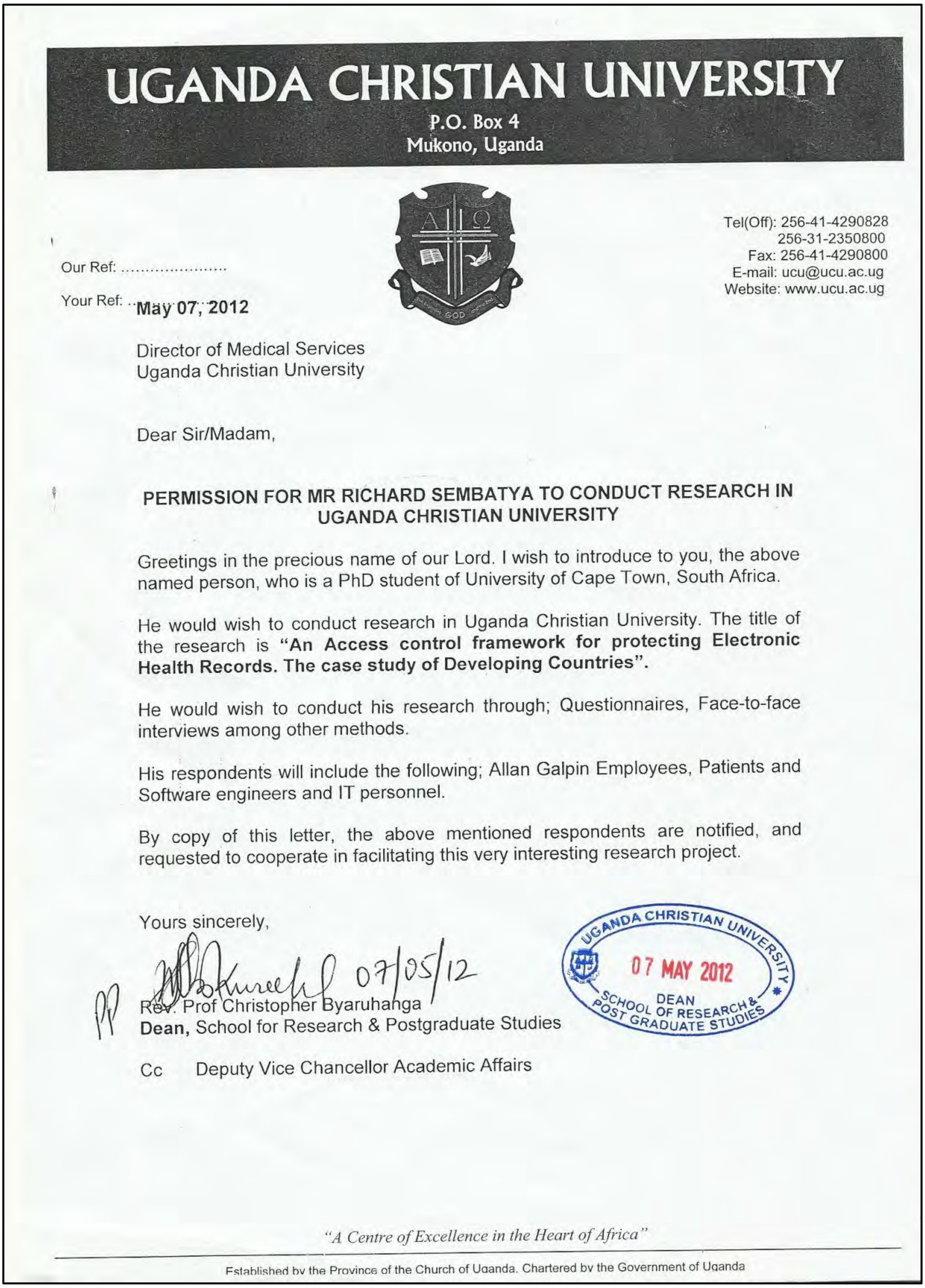
Your approval code is: SFREC 015_2012

I wish you success in the work involved.

Yours sincerely

M Meadows

Michael E Meadows
Professor and Head of Department
Chair: Science Faculty Ethics in Research Committee



UGANDA CHRISTIAN UNIVERSITY
P.O. Box 4
Mukono, Uganda

Tel(Off): 256-41-4290828
256-31-2350800
Fax: 256-41-4290800
E-mail: ucu@ucu.ac.ug
Website: www.ucu.ac.ug

Our Ref: ....

Your Ref: ...**May 07, 2012**

Director of Medical Services
Uganda Christian University

Dear Sir/Madam,

PERMISSION FOR MR RICHARD SEMBATYA TO CONDUCT RESEARCH IN UGANDA CHRISTIAN UNIVERSITY

Greetings in the precious name of our Lord. I wish to introduce to you, the above named person, who is a PhD student of University of Cape Town, South Africa.

He would wish to conduct research in Uganda Christian University. The title of the research is **"An Access control framework for protecting Electronic Health Records. The case study of Developing Countries".**

He would wish to conduct his research through; Questionnaires, Face-to-face interviews among other methods.

His respondents will include the following; Allan Galpin Employees, Patients and Software engineers and IT personnel.

By copy of this letter, the above mentioned respondents are notified, and requested to cooperate in facilitating this very interesting research project.

Yours sincerely,

pp 07/05/12

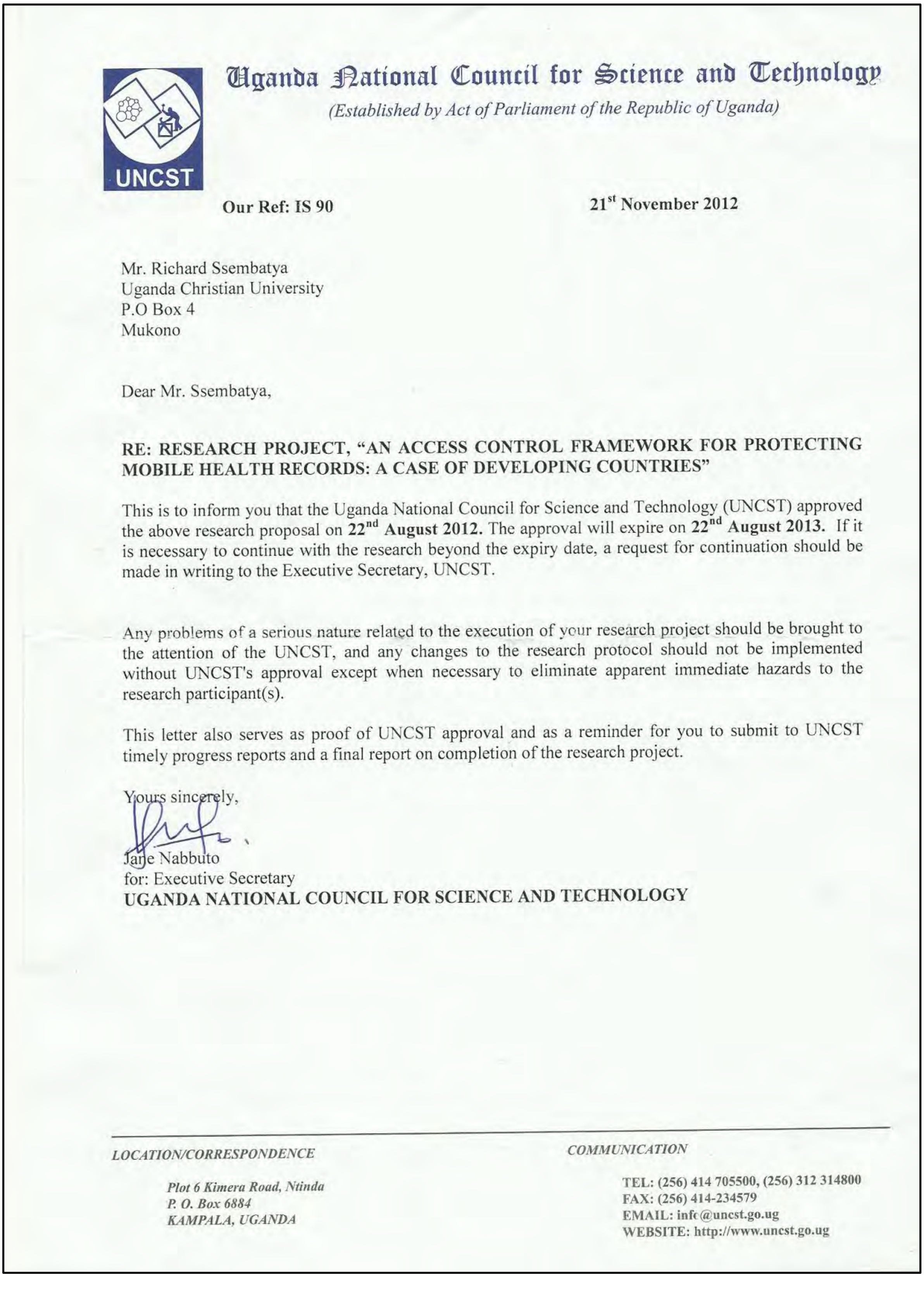
Rev. Prof Christopher Byaruhanga
Dean, School for Research & Postgraduate Studies

UGANDA CHRISTIAN UNIVERSITY
07 MAY 2012
DEAN
SCHOOL OF RESEARCH & POST GRADUATE STUDIES

Cc Deputy Vice Chancellor Academic Affairs

"A Centre of Excellence in the Heart of Africa"

Established by the Province of the Church of Uganda. Chartered by the Government of Uganda



Uganda National Council for Science and Technology

(Established by Act of Parliament of the Republic of Uganda)

UNCST

Our Ref: IS 90 **21st November 2012**

Mr. Richard Ssembatya
Uganda Christian University
P.O Box 4
Mukono

Dear Mr. Ssembatya,

RE: RESEARCH PROJECT, "AN ACCESS CONTROL FRAMEWORK FOR PROTECTING MOBILE HEALTH RECORDS: A CASE OF DEVELOPING COUNTRIES"

This is to inform you that the Uganda National Council for Science and Technology (UNCST) approved the above research proposal on **22nd August 2012.** The approval will expire on **22nd August 2013.** If it is necessary to continue with the research beyond the expiry date, a request for continuation should be made in writing to the Executive Secretary, UNCST.

Any problems of a serious nature related to the execution of your research project should be brought to the attention of the UNCST, and any changes to the research protocol should not be implemented without UNCST's approval except when necessary to eliminate apparent immediate hazards to the research participant(s).

This letter also serves as proof of UNCST approval and as a reminder for you to submit to UNCST timely progress reports and a final report on completion of the research project.

Yours sincerely,

Jane Nabbuto
for: Executive Secretary
UGANDA NATIONAL COUNCIL FOR SCIENCE AND TECHNOLOGY

LOCATION/CORRESPONDENCE

Plot 6 Kimera Road, Ntinda
P. O. Box 6884
KAMPALA, UGANDA

COMMUNICATION

TEL: (256) 414 705500, (256) 312 314800
FAX: (256) 414-234579
EMAIL: info@uncst.go.ug
WEBSITE: http://www.uncst.go.ug

APPENDIX 4.1: PATIENTS SURVEY TO DETERMINE THEIR REQUIREMENTS AND NEEDS

You can help us learn more about your experience with Personal Health Record (PHR) by completing this survey. Your participation is voluntary and your healthcare at Allan Galpin Health Centre (AGHC) will not be affected if you do not participate in the survey. The information you provide will remain **STRICTLY CONFIDENTIAL**. The survey responses will be aggregated and only a summary will be reported. The results will be used only for research purposes to determine how the current system works, and the state of PHR services at AGHC. Please provide as accurate and honest an answer as possible to each question.
Thank you for your time and cooperation.

Demographics

Age: 15 – 19 □ 20 – 24 □ 25 – 29 □ 30 – 34 □ 35 – 39 □ 40&Above □

Gender: Male □ Female □

Highest Qualification: None □ Primary level □ Secondary level □ Tertiary □

- How often do you visit a health service provider?
- When you visit the health service provider, what kind of information are you always required to provide other than information about your illness
- Do you worry about someone else looking at your records
- Would you like more information about your stay in hospital when you leave?
    1. If yes, what would you like?
    2. How would you want to see the information?
- Would you like to keep or be in charge of your medical records?
- How would you feel if your medical records can be shared across different health service providers such that you don't have to explain yourself every time you visit a different provider?

    If ok,

    - What information would you like to share?
- Do you know what health providers call electronic health records?
- Would you be willing to use your personal device in storing and sharing your medical records?
- Do you have any idea about keeping "stuff" private on personal devices?

- How would you feel about having your records on a personal device?
- Which personal device would you prefer?
- Is there any information which you would prefer not to be stored on the device specified above?

APPENDIX 4.2: HEALTHCARE GIVERS SURVEY TO DETERMINE HOW THE CURRENT HEALTHCARE SYSTEM WORKS, UNDERSTAND PHRs, CHALLENGES AND OPPORTUNITIES

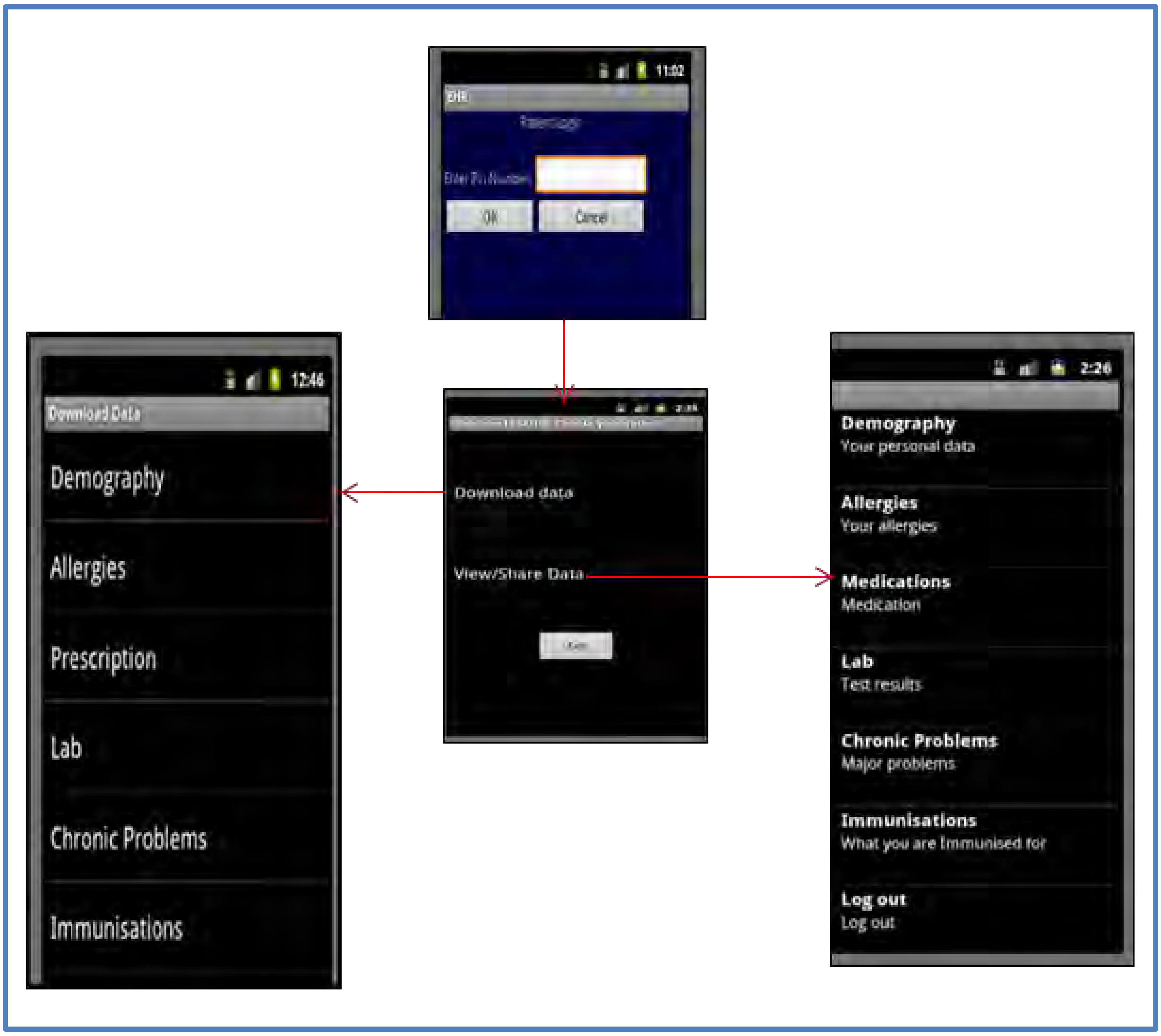
You can help us learn more about Personal Health Record (PHRs), and your experiences with the current healthcare system by completing this survey. Your participation is voluntary and will not affect your work. The information you provide will remain **STRICTLY CONFIDENTIAL**. The survey responses will be aggregated and only a summary will be reported. The results will be used only for research purposes to determine: how the current system works; opportunities and challenges, and the structure of PHRs. We would like a few minutes of your time to have you answer the survey questions below. Thank you for your time, and participating in this survey.

Date: ____

Title: ____

1. Do you receive sufficient information on your patient's stay?
2. Do you receive the information in a timely fashion?
3. Does the patient carry out appropriate self-care or often require readmission to the health centre?
4. Do you think that the care of patients would be improved if your patient or you had more information about their stay at the health centre?
5. What kind of information would you like to see made available to the patients?
6. What are some of the challenges that you regularly experience when a patient visits your healthcare?
7. How have you been handling these challenges?
8. Do you think that electronic personal health records would overcome some of these challenges?
9. Do you think that device-based PHRs would enhance the patient's perception of communication?
10. In terms of patient confidentiality, what information the patient can have on a personal device such as a mobile phone?
11. What are your greatest concerns about the patient having access to mobile phone-based records?
12. Do you have any other suggestions?

APPENDIX 4.3: THE SCREEN SHOTS OF THE INITIAL HIGH-FIDELITY PROTOTYPE



APPENDIX 4.4: INTERVIEW GUIDE USED BY PATIENTS TO EVALUATE THE INITIAL PROTOTYPE

Section A: **General Information**

Instruction

The following grade scale is used

- **A. Strongly Agree**
- **B. Agree**
- **C. Disagree**
- **D. Strongly disagree**

Please tick the grade scale that applies to every statement in your opinion

	A	B	C	D
1. The system can be used without thinking	□	□	□	□
2. Terminologies related to the task is not understandable	□	□	□	□
3. The sequence of screens are confusing	□	□	□	□
4. Performing tasks are not straight forward	□	□	□	□
5. The system icons does not relate to the functions	□	□	□	□
6. You can explore the system features using trial and error	□	□	□	□

	A	B	C	D
7. The system is easy to use	□	□	□	□
8. It is not easy to navigate the system	□	□	□	□
9. The system is enjoyable to use	□	□	□	□
10. The system is easy to learn after training	□	□	□	□

	A	B	C	D
11. The system may make sharing my records easier	□	□	□	□
12. The system functions facilities the easy with which my records can be shared	□	□	□	□
13. It is easy to understand the features provided by the system	□	□	□	□

Comments

List the areas where you would want to see improvement on this new technology

1……………………………………………………………………………………………….

2………………………………………………………………………………………………..

3………………………………………………………………………………………………..

APPENDIX 4.5: FOCUS GROUP (PATIENT ACCESS TO THE INITIAL HIGH-FIDELITY PROTOTYPE)

<u>These questions will guide the focus group discussion.</u>

1. Were you able to access you records using M-Health App system?
2. How did you do it?
3. What challenges did you face?
4. How did you overcome these challenges?
5. Did you understand the system?
6. Does the system work as you would like to work?
7. Do you think the system capture all your needs?
8. Are the need and requirements represented well in the system?
9. Are there any preferences to the system used?
10. Where would you want to see changes proposed? Why? Tell me more about this?

Date: Tuesday, 24 July 2012

The Dean,
School for Research and Postgraduate Studies,
Uganda Christian University

Dear Prof,

Vote of Thanks

Greetings in the name of our Lord Jesus Christ!

I wish to take this opportune moment to convey my heartfelt thanks for the opportunity you gave me and conduct my fieldwork at *Allan Galpin Health centre*. The staff at *Allan Galpin Health centre* were so gracious and easy to work with throughout this first phase of my research.

Special thanks go to Ms Christine (Clinical officer) for her time, information and guidance during the interview. Thank you Christine. Your information has enabled me improve the M-health application. **Working with you was a very enlightening experience for me.** Hope for your continued support.

My second phase of evaluation (Nov 2012 – February 2013) will involve deploying the applications (server based and mobile phones applications) for evaluations. I will involve patients and healthcare professionals (at A*llan Galpin Health Clinic*) to evaluate the application and give further recommendations. I look forward for your continued support.

God bless you.

Yours faithfully,

Richard Ssembatya
Researcher
HPI Research School in ICT4D Centre
University of Cape Town

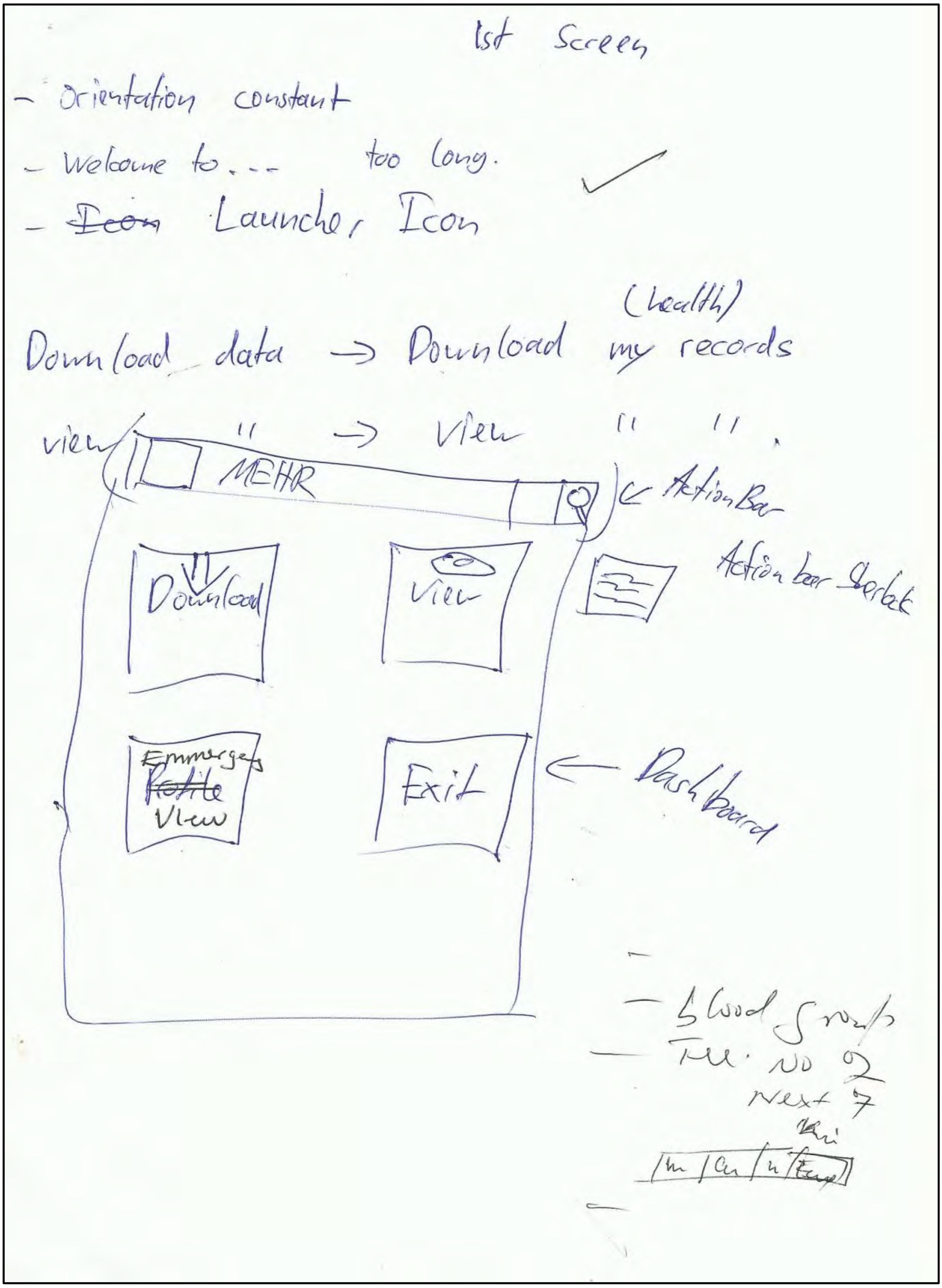
C.c. Director, *Allan Galpin Health Centre*
C.c. Ms Christine Namatovu – Clinical Officer

APPENDIX 6.1: NOTATION USED IN M-HEALTH APP PHR SYSTEM

Table: 6.2: Symbolic representation of jpair operations

Nos.	Symbol	Representation
1.	EC	Elliptic Curve: $y^2 = x^3 + x$ defined over the field F_p
2.	F_p	The field where the Elliptic Curve (EC) is constructed, with q where q = 3 mod 4
3.	p	The generator of the EC group
4.	s	Master secret of the PKG.(An arbitrary element of $\mathbb{Z}_q^*$)
5.	$qbits$	The bits which we use fir the prime number q
6.	$rbits$	The bits of prime number r.
7.	ID	An arbitrary string over $\{0, 1\}^*$
8.	sP or $Ppub$	The scalar multiplication of s with P (public key of the PKG)
9.	$\hat{e}(P_1, P_2)$	The bilinear pairing between the P_1 (point of the EC) and P_2 (point of the EC)
10.	Qid	A point on EC calculated from ID
11.	$sQid$	The scalar multiplication of s with the Qid (private key)
12.	H_1	The hash function which maps ID to Qid
13	r	An arbitrary element of $\mathbb{Z}_q^*$
14	rP	The Scalar multiplication of r with P
15	$\|$	String concatenation

APPENDIX 7.1: THE DESCRIPTION OF HEURISTIC ILLUSTRATIONS OBTAINED FROM HEURISTIC EVALUATION



1st Screen

- orientation constant
- welcome to... too long. ✓
- ~~Icon~~ Launcher, Icon

Download data → Download (health) my records

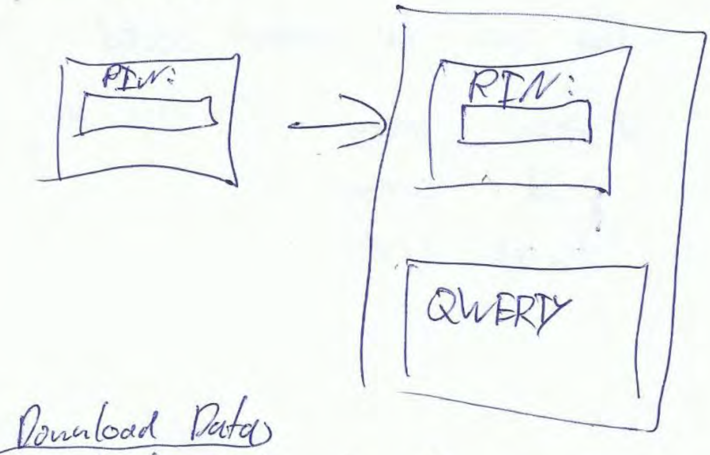
view " → View " ".

MEHR
Action Bar
Action bar Sherlok
Download
View
~~Emmergey~~
~~Profile~~
View
Exit
Dashboard

-
- blood group
- Tel. No 9
Next 7
[illegible]
-

m / Cn / n / [illegible]

Download

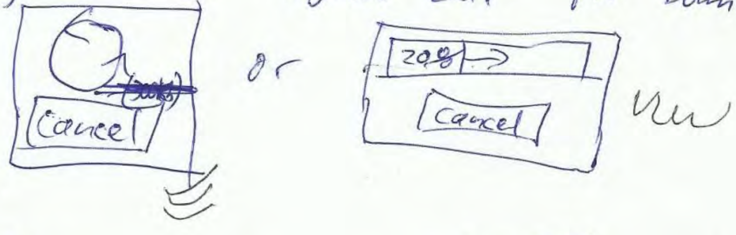


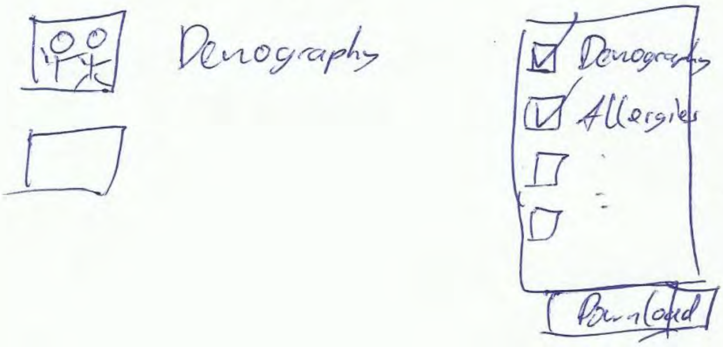
Fn TextView
No predictive text

Download Data
Select Data to Download:

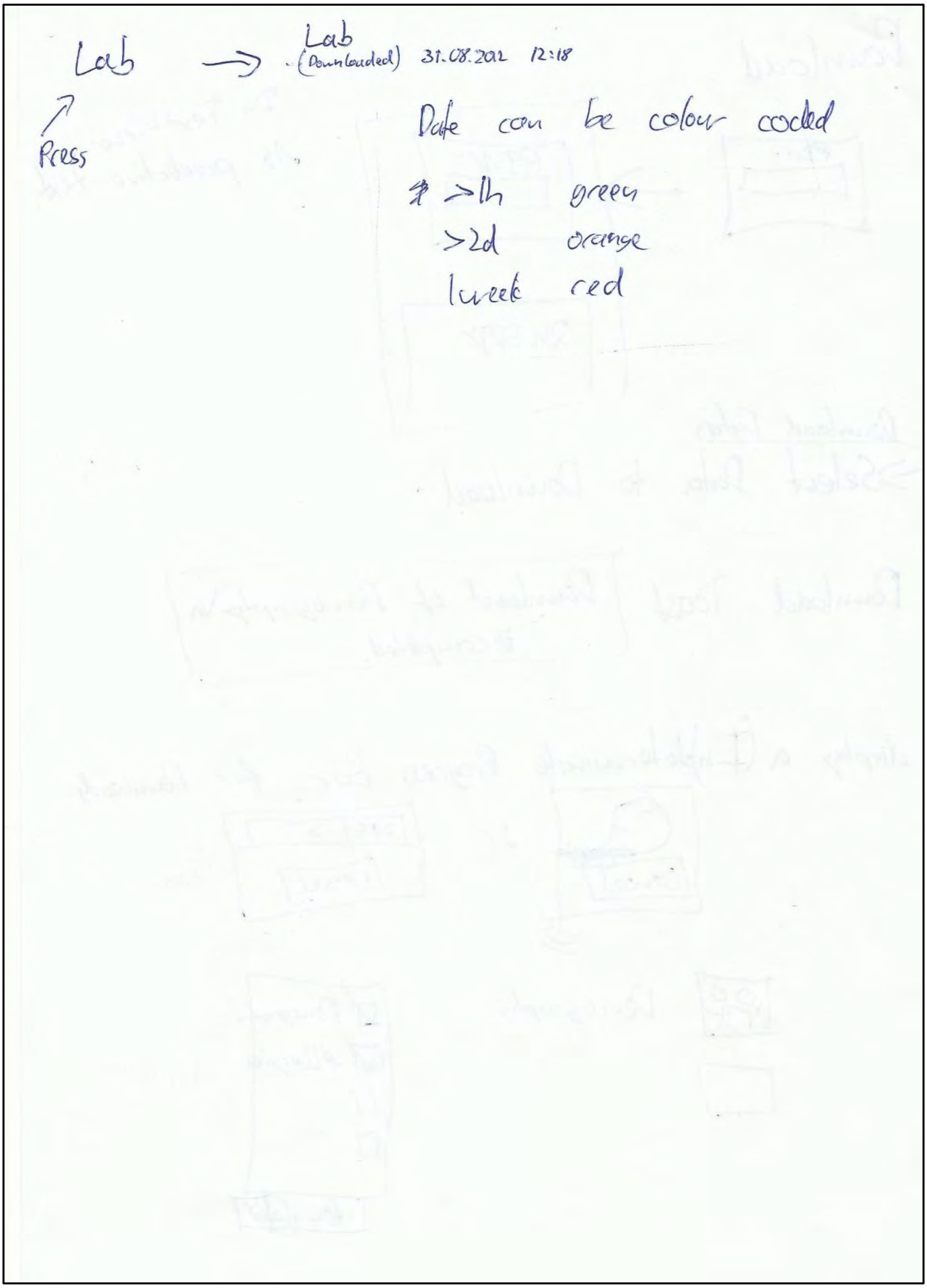
Download Toast | Download of Demography \n ~~B~~ completed.

display a (In)determinate Progress Bar for Downloads





Done

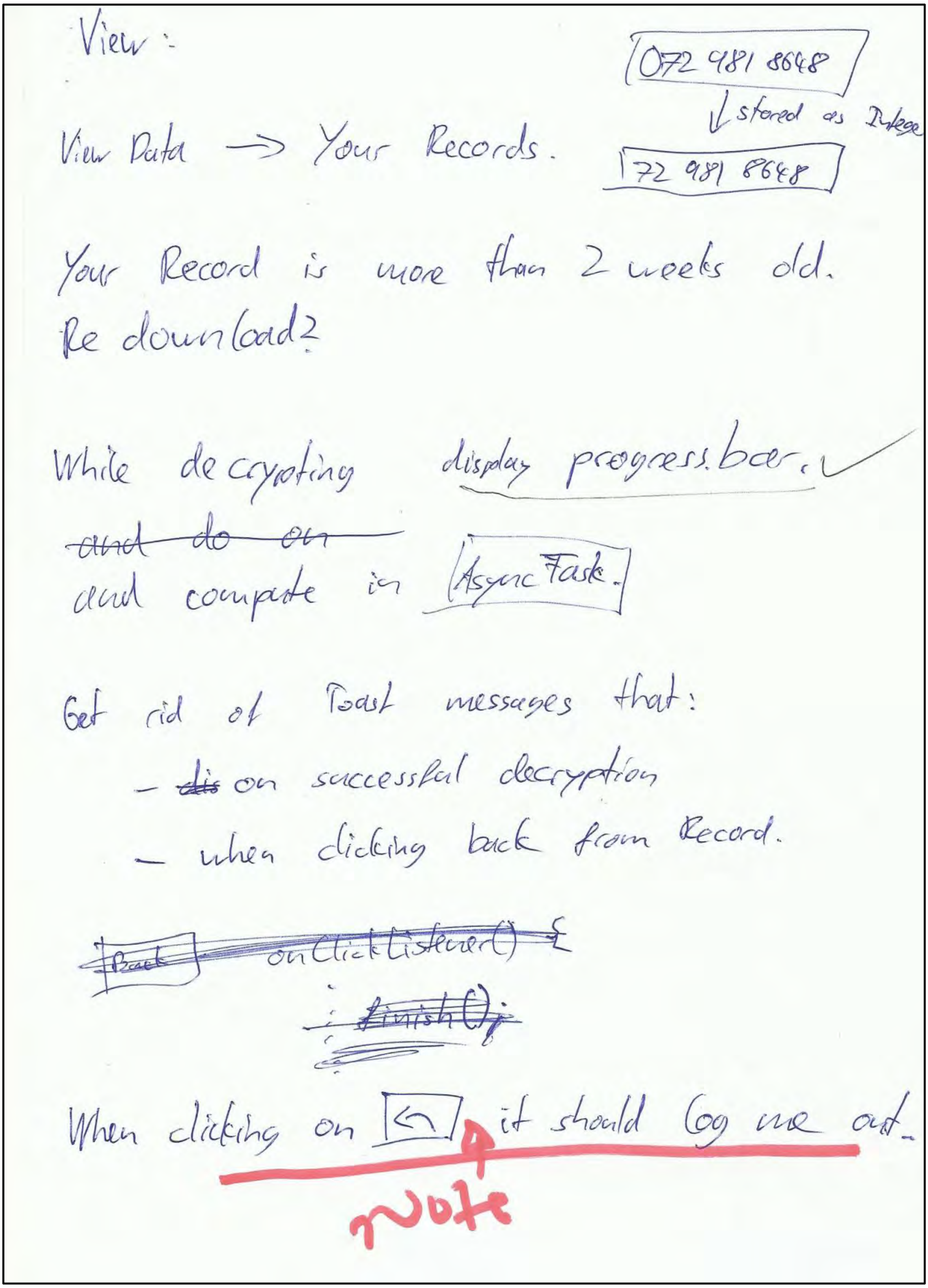


Lab → Lab (Downloaded) 31.08.2022 12:18

Press

Date can be colour coded

>1h	green
>2d	orange
1week	red



View:

072 981 8648

↓ stored as Intege

72 981 8648

View Data → Your Records.

Your Record is more than 2 weeks old.
Re download?

While decrypting display progress bar. ✓

~~and do on~~
and compute in AsyncTask.

Get rid of Toast messages that:

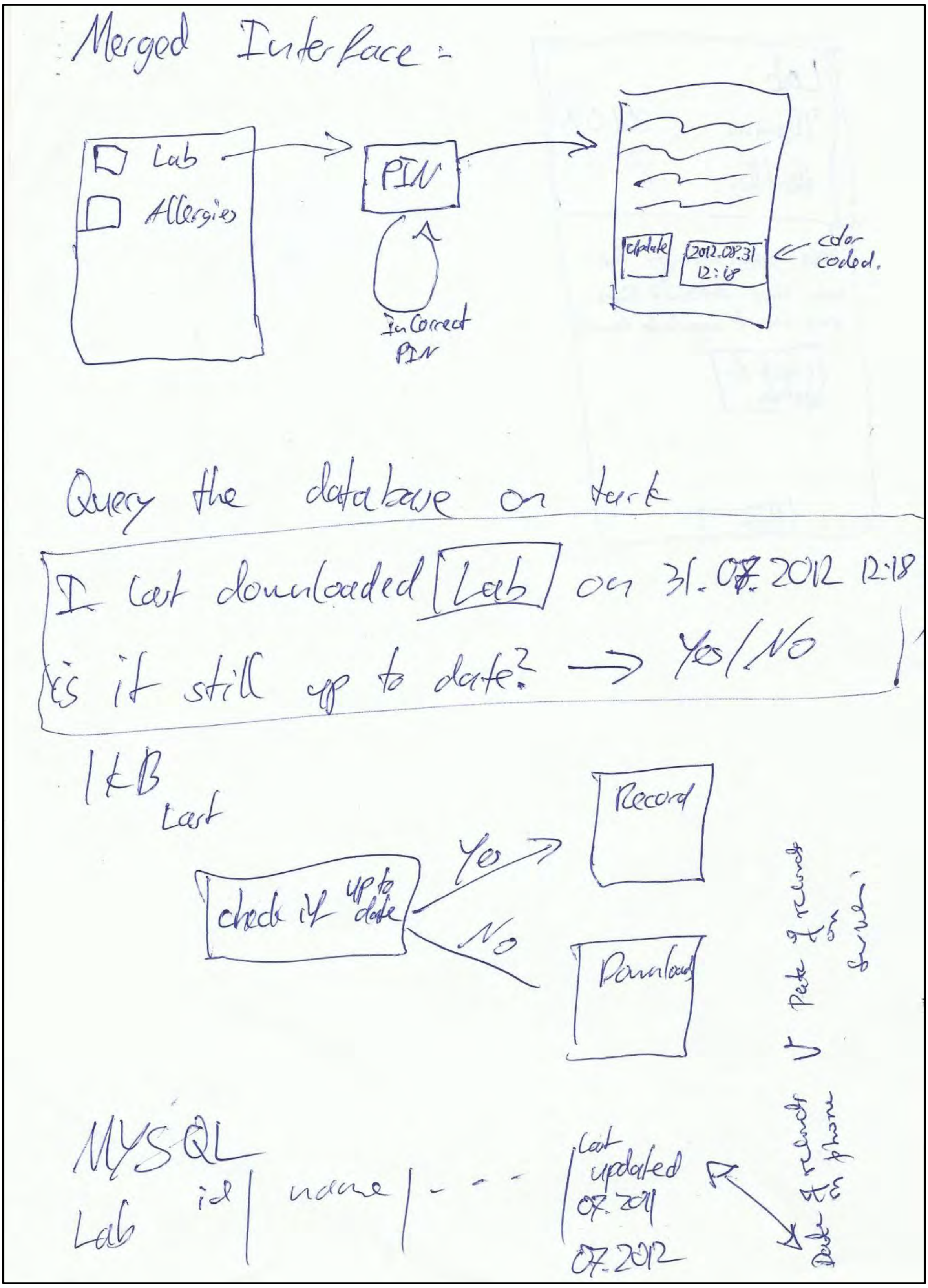
- ~~dis~~ on successful decryption
- when clicking back from Record.

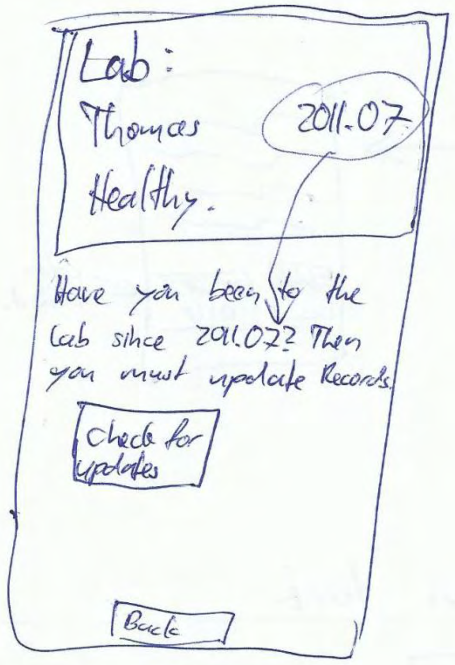
~~Back onClickListener() {~~

~~finish();~~

When clicking on ↩ it should log me out.

note

Merged Interface:
Lab
Allergies
PIN
Incorrect PIN
update
2012.08.31 12:18
color coded.
Query the database on task
I last downloaded Lab on 31.07.2012 12:18
is it still up to date? → Yes/No
IKB last
check if up to date
Yes
No
Record
Download
Part of refresh on server
MYSQL
Lab
id
name
- - -
last updated
07.2011
07.2012
Date of refresh on phone



Have you been to the lab since 2011.07? Then you must update Records

APPENDIX 7.2: USABILITY FACTORS AND EMPIRICAL MEASUREMENTS

(Guillemette, RA (1995), Lindgaard, G. (1994), Nielsen, J. (1993))

Factors	Objective Measures	Subjective Measures
Efficiency: Productive once users have learned the system	Time taken to accomplish the tasks once users have learned the system	User's ratings of the system's ability to improve the way at which they provide EHRs to healthcare professionals
Effectiveness: Usefulness for supporting intended tasks	Successful performance of the intended tasks, it is the measure of productivity	User's ratings of the system's ability to promote their performance and productivity
User Satisfaction: Pleasant for users	Frequency of utilisation of the system and its features	User's ratings of their perceptions and opinions of the system and its features
Learnability: Ease with which the use of the application is learned so that users can rapidly accomplish intended tasks	Time taken by new users to learn and accomplish the intended tasks	User's ratings of the ease and time to learn the system
Memorability: Ease with which casual users can return to the system without having to relearn	Memory failure rate on how to use the system the next time .i.e. Time to re-learn the system after periods of non-use	User's ratings of the ability to remember how to use the system the next time and their ability to re-learn the system after periods of non-use
Errors: Low frequency of errors and easy recovery	Error rates trying to use the system.	User's ratings of the impact of errors on using the system and their ability to recover from errors

APPENDIX 7.3: WAITING TIME TO DOWNLOAD THE RECORDS FROM THE SERVER TO MOBILE PHONE

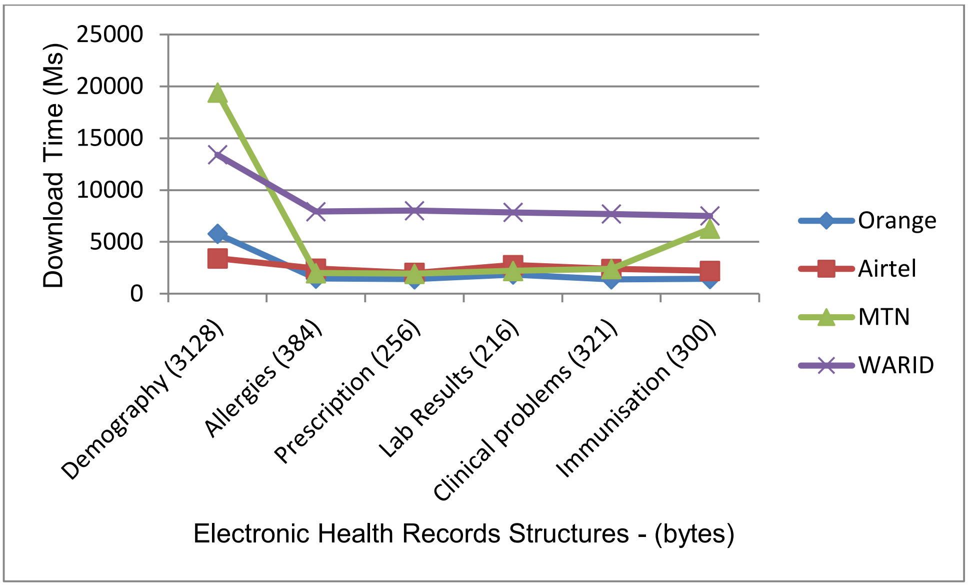


Figure 7.3 (a): Download time at Mukono – 8:30-11:30am

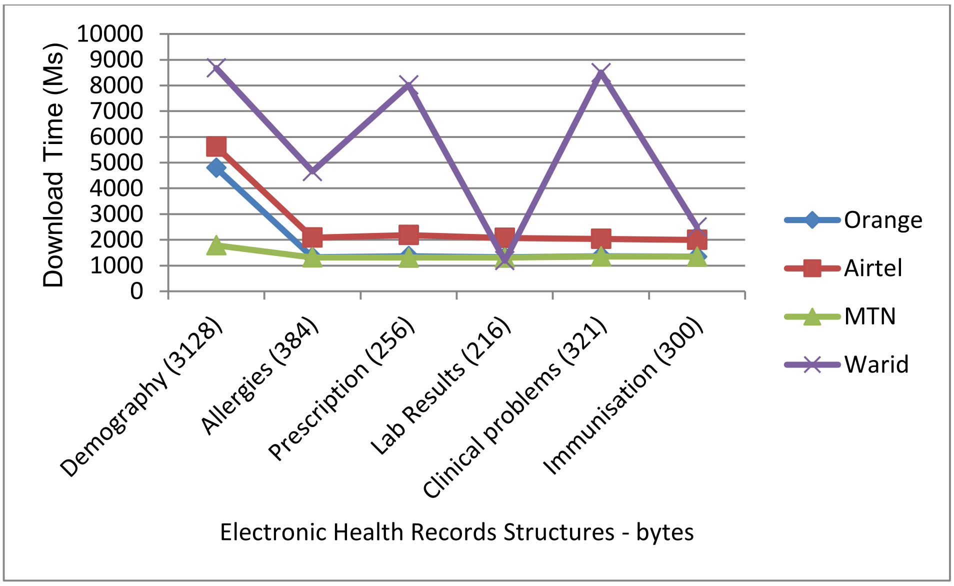


Figure 7.3 (b): Download time at Mukono – 12:30-4:00pm

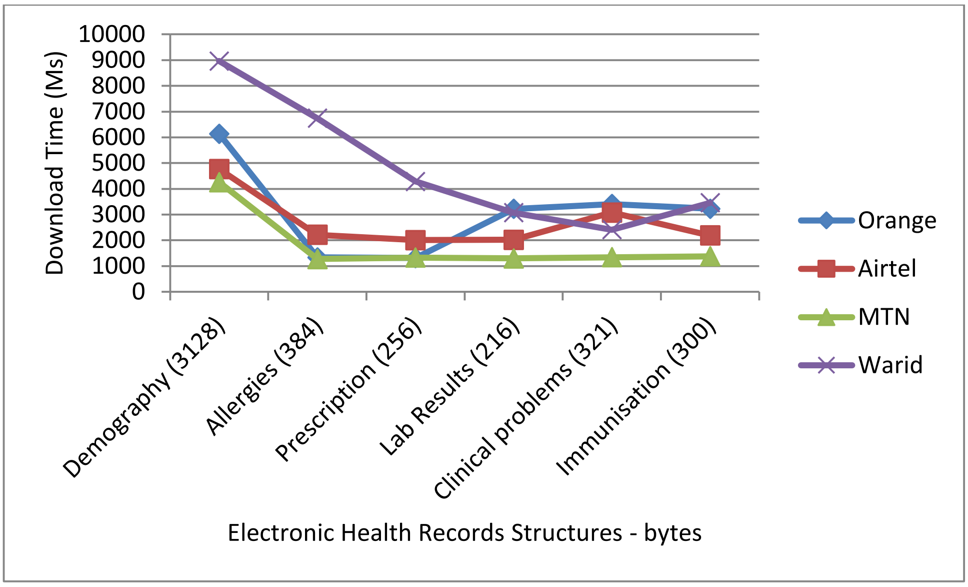


Figure 7.3 (c): Download time at Mukono – 4:30-8:30pm

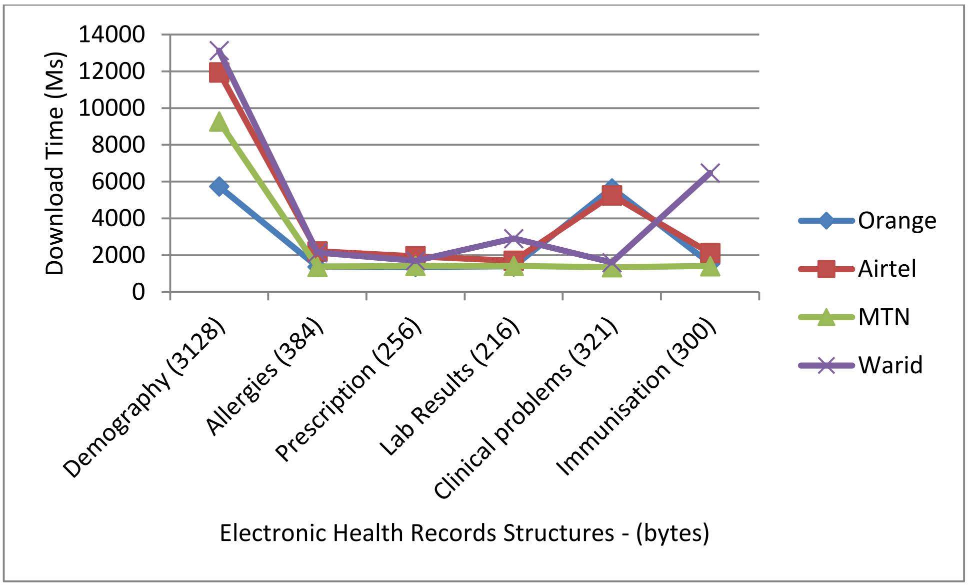


Figure 7.3 (d): Download time at Buddo – 8:30-11:30am

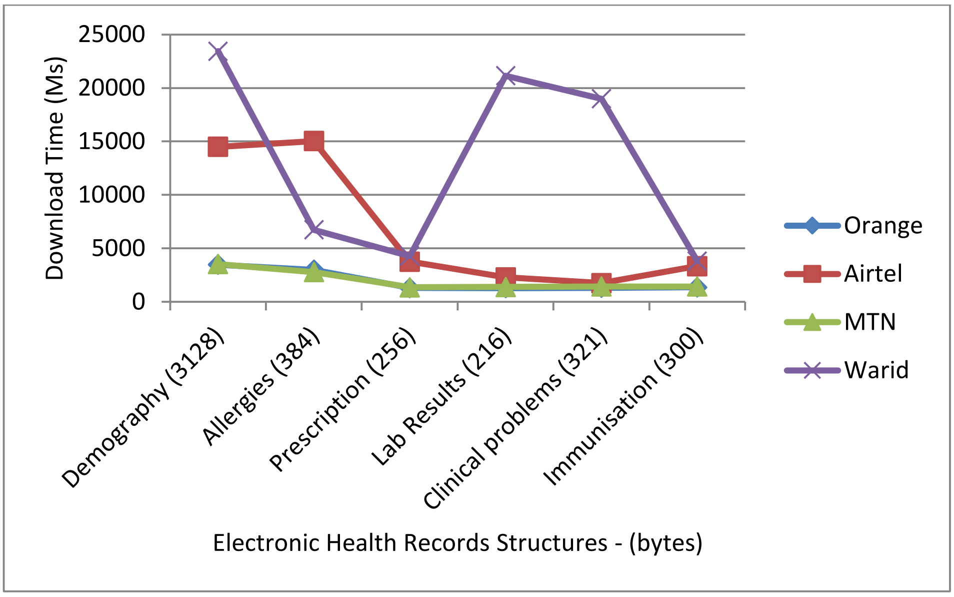


Figure 7.3 (e): Download time at Buddo – 12:30-4:00pm

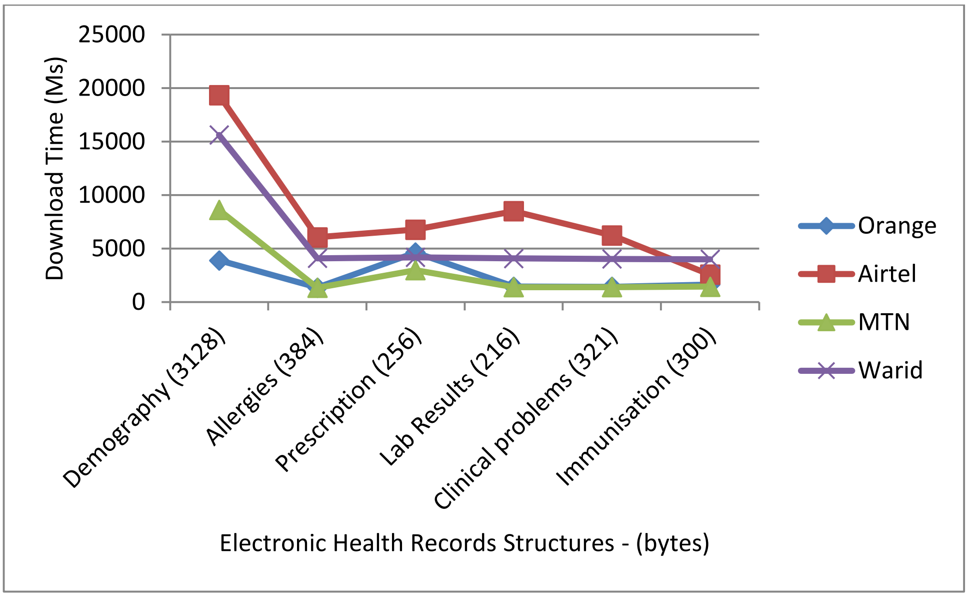


Figure 7.3 (f): Download time at Buddo – 4:30-8:30pm

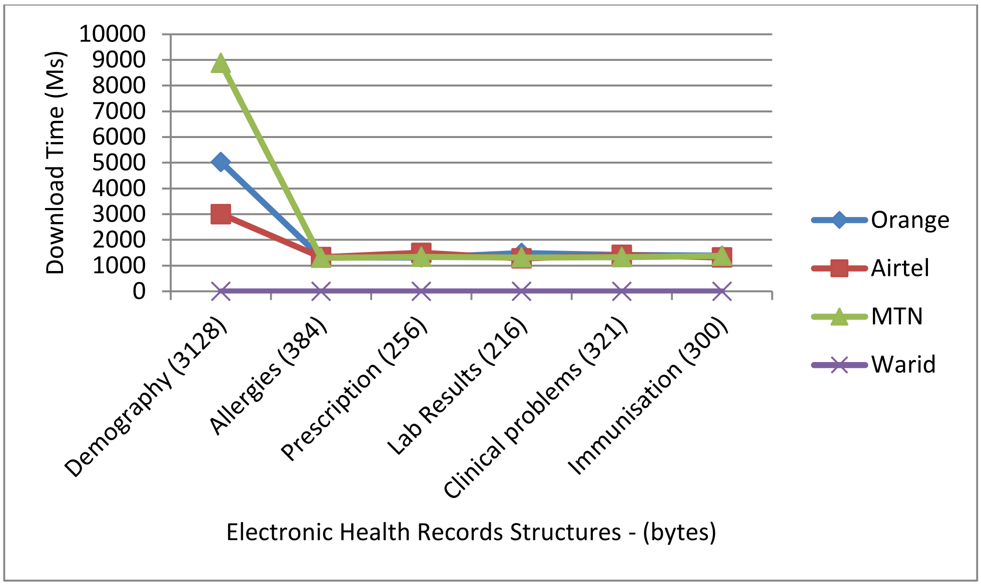


Figure 7.3 (g): Download time at old Kampala – 8:30-11:30am

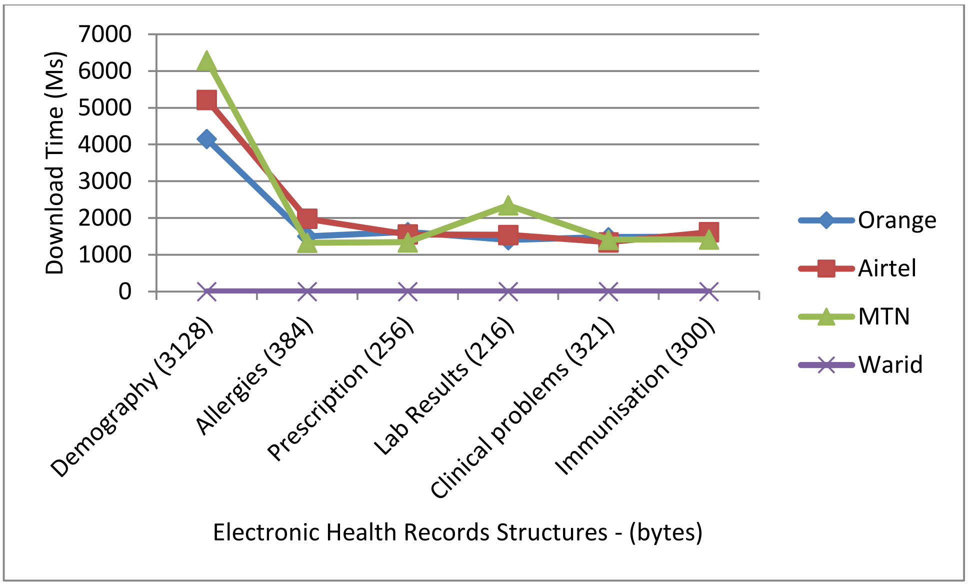


Figure 7.3 (h): Download time at old Kampala – 12:30-4:00pm

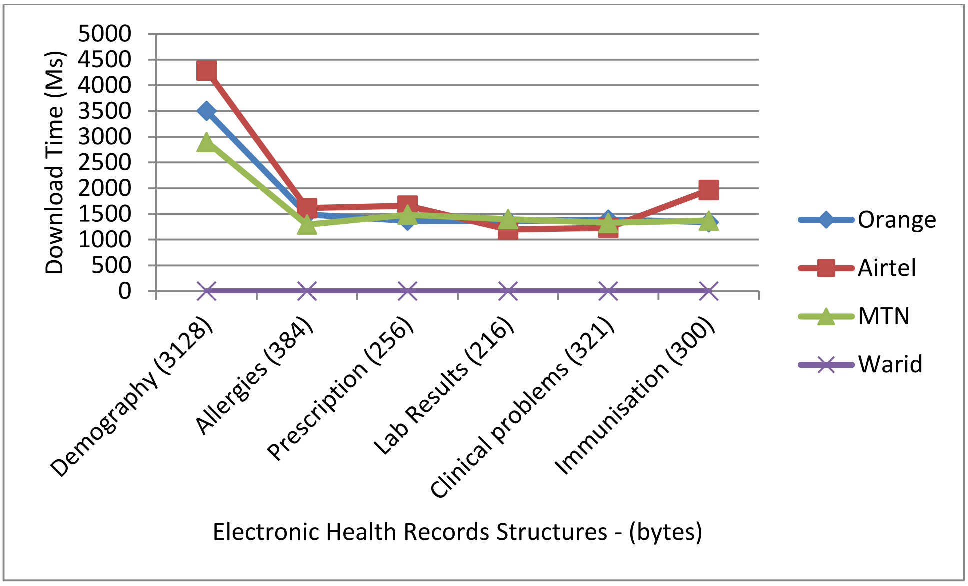


Figure 7.3 (i): Download time at old Kampala – 4:30-8:30pm

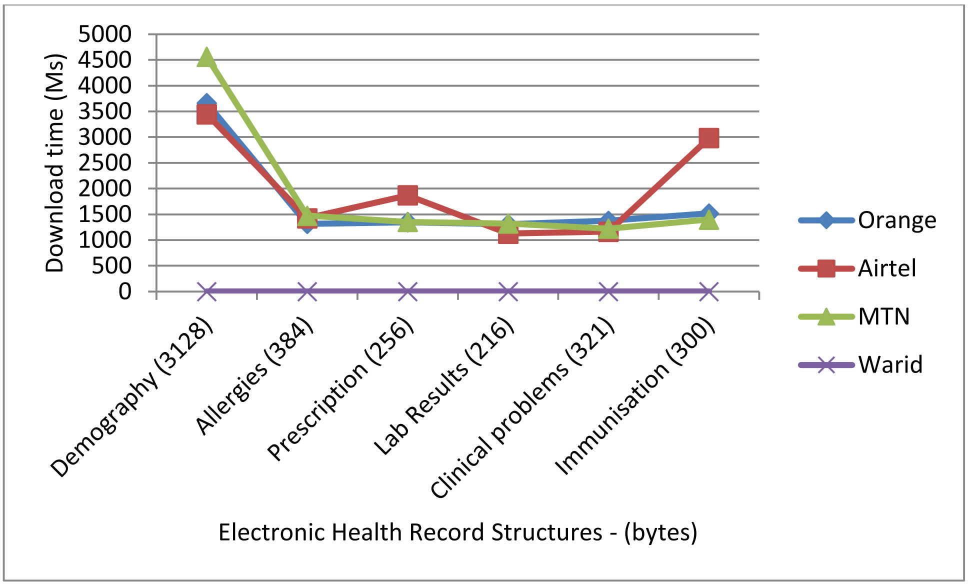


Figure 7.3 (j): Download time at Nsangi – 8:30-11:30am

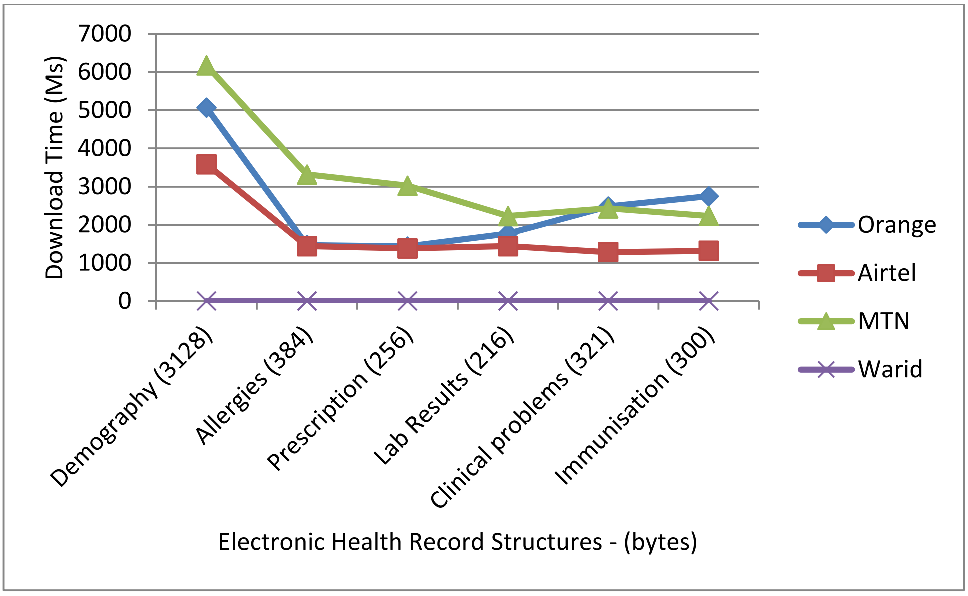


Figure 7.3 (k): Download time at Nsangi – 12:30-4:00pm

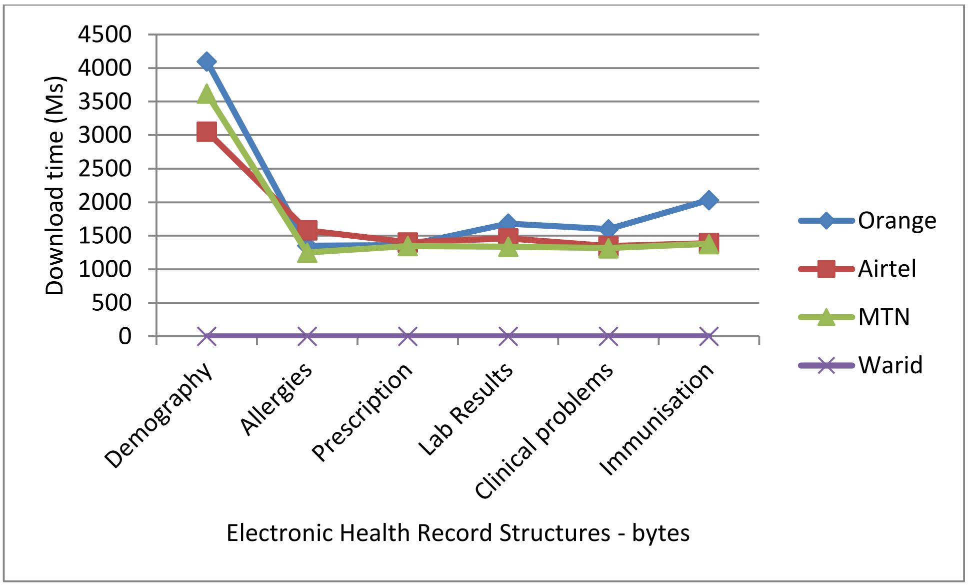


Figure 7.3 (l): Download time at Nsangi – 4:30-8:30pm

APPENDIX 7.4: THE POST-STUDY SYSTEM USABILITY QUESTIONNAIRE

Dear participant, the questionnaire is designed to give you an opportunity and tell us your reactions of the M-Health App you used. Your response will help us understand what features\functionalities of the system that you are particularly concerned about and those with which you are satisfied. You are requested to think about all the tasks that you have performed with the system as you are answering these questions.

Please read each question and indicate how strongly you agree or disagree with the question by circling a number on the scale. For any question that does not apply to you, circle N/A. You are encouraged to elaborate your answers under comments. We will go over your responses with you after completing this questionnaire to ensure that we understand all your responses. Thank you so much.

Demographics

Age: 15 – 19 □ 20 – 24 □ 25 – 29 □ 30 – 34 □ 35 – 39 □ 40&Above □

Gender: Male □ Female □

Highest Qualification:

None □

Primary level □

Secondary level □

Vocational □

Tertiary □

Others (Specify) □

Mobile device use:

Mobile phone □

Laptop □

Personal Digital Assistant (PDA) □

Previous mobile application used:

Standalone application (e.g. Calendar, calculator) □

Network enabled application (e.g. Warid pesa) □

Electronic health application □

1. This system has all the functions and capabilities I expect it to have.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

2. Overall, I am satisfied with this system.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

3. Overall, I am satisfied with how easy it is to use this system
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

4. It was simple to use this system
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

5. I could effectively complete the tasks and scenarios using this system.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

6. I was able to complete the tasks and scenarios quickly using the system.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

7. I was able to efficiently complete the tasks and scenarios using this system.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

8. I felt comfortable using this system.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

9. It was easy to learn and to use this system
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: …………………………………………………………………....

10. The interfaces of this system were pleasant.

Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

11. I liked using the interfaces of this system
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

12. The organisation of information on the system screens was clear
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

13. The system gave error messages that clearly told me how to fix problems
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

14. Whenever I made a mistake using the system, I could recover easily and quickly.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

15. It was easy to find information I needed.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

16. The information provided for by the system was easy to understand
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

17. The information was effective in helping me complete the tasks and scenarios.
Strongly Agree Strongly disagree Not Applicable
1 2 3 4 5 6 7 N/A
Comments: ……………………………………………………………….....

APPENDIX 7.5: INFORMED CONSENT AGREEMENT

This is to certify that I

____

Have agreed to work with Richard Ssembatya on a research project he is conducting under the University of Cape Town in conjunction with *Allan Galpin Health Centre*. I agree to receive from the project a Google IDEOS handset that will be used to give me access to my personal health information. I understand that what is expected of me in this project is to give my opinions on the system. I hereby grant him the permission to publish these opinions and other observations in his research papers and thesis. He may use my pictures in his thesis and publications. I am aware that I have the right to opt out of this research at any time. I promise to return the handset any time it is needed.

Signature: ___________________________ Date: _______________________