A SECURE APPROACH FOR HEALTH INFORMATION EXCHANGE USING MOBILE PERSONAL HEALTH RECORDS

MOHAMED SHABBIR HAMZA ABDULNABI

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

A SECURE APPROACH FOR HEALTH INFORMATION EXCHANGE USING MOBILE PERSONAL HEALTH RECORDS

MOHAMED SHABBIR HAMZA ABDULNABI

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: MOHAMED SHABBIR HAMZA ABDULNABI

Matric No: WHA120046

Name of Degree: DOCTOR OF PHILOSOPHY

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"): A SECURE APPROACH FOR HEALTH INFORMATION EXCHANGE USING MOBILE PERSONAL HEALTH RECORDS

Field of Study: COMPUTER SECURITY (COMPUTER SCIENCE)

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 03/05/2018

Subscribed and solemnly declared before,

Witness's Signature Date: 03/05/2018

Name: PROF.DR.MISS LAIHA MAT KIAH

Designation: SUPERVISOR

A SECURE APPROACH FOR HEALTH INFORMATION EXCHANGE USING MOBILE PERSONAL HEALTH RECORDS

ABSTRACT

Sharing patient information between different care providers has been identified early as a key enabler for quality and cost-effective healthcare. Being in the information age, it seems natural to expect immediate access to health information in the right place at the right time and in a usable format. However, the realization of such vision is taking too long, and the level of providers' engagement is witnessing a decline. Difficulties in ensuring global connectivity, interoperability and concerns on security have always hampered attempts by the governments to deploy nationwide Health Information Exchange (HIE) successfully. An important question to pose is how new approaches can address the same issues of interoperability and interconnectivity without disturbing existing infrastructure and imposing much costs. Bearing in mind the pervasiveness and power of modern smartphones, this thesis proposes an alternative approach for nationwide HIE that can replace or complement governmental efforts, such as the Malaysian MyHIX project. The main objective is to introduce the idea of a multi-component and distributed solution for large-scale HIE as a novel approach that differs from the existing central approaches but does not disturb the current set-up and attribute no significant costs to any of the involved stakeholders. The proposed approach provides a distributed framework in which patient data are carried by the patients themselves in the form of mobile Personal Health Records (mPHRs), typically on their handheld smartphones. This method uses the concept of mPHR in a novel way –as distributed storage units– and is to be compared with the current central approaches that aim to collect patient data in central repositories and circulate them via central engines. The individual mPHR systems are capable of interconnecting securely with multiple

healthcare systems through a suitable interface. This interface is another app that runs on a special terminal device (such as a tablet) at the end of the healthcare system to ensure the interoperability with the patients' smartphones. The detailed design and operation of the proposed approach is provided and justified, resulting in a multi-component and coherent framework for HIE. The proposed framework consists of three main components: an mPHR at the side of the patient, legacy Health Information System (HIS) at the side of healthcare providers, and an interface device between the two. The whole framework is validated through a prototype implementation using software apps for the mPHR and the interface layer, and open source Electronic Medical Record (EMR) systems to represent legacy HISs used by healthcare providers. Various simulated use cases and scenarios have been presented to show the operation of the framework and its overall validity. Endorsement of the proposed framework can lead to a practical solution to the hard problem of HIE that avoids the cost of implementing a single global network to connect all healthcare systems, and ensures that the required data of each patient is available whenever and wherever it is needed.

Keywords: health information exchange, bioinformatics, NFC, mobile computing, mPHR

A SECURE APPROACH FOR HEALTH INFORMATION EXCHANGE USING MOBILE PERSONAL HEALTH RECORDS

ABSTRAK

Berkongsi maklumat pesakit antara pembekal penjagaan kesihatan (care providers) yang berbeza telah dikenal pasti dari awal sebagai penyumbang utama untuk penjagaan kesihatan yang berkualiti dan kos efektif. Di zaman maklumat kini, sudah menjadi kebiasaan untuk mengharapkan capaian pantas terhadap maklumat kesihatan pada tempat dan masa yang tepat, dan dalam format yang boleh digunakan. Namun, untuk merealisasikan visi tersebut mengambil masa yang lama, dan tahap penglibatan para pembekal menunjukkan penurunan. Kesukaran dalam memastikan kesalinghubungan global, kebolehoperasian, dan kebimbangan terhadap keselamatan seringkali menghalang percubaan kerajaan untuk menyebarkan Pertukaran Maklumat Kesihatan (HIE) di seluruh negara. Satu persoalan penting yang perlu dipertimbangkan adalah bagaimana pendekatan baru dapat menangani masalah yang sama antara kebolehoperasian dan kesalinghubungan tanpa menganggu infrastruktur yang sedia ada dan mengenakan banyak kos. Dalam mempertimbangkan kuasa dan penggunaan telefon pintar moden yang meluas, tesis ini mencadangkan pendekatan alternatif untuk HIE di seluruh negara yang dapat menggantikan atau melengkapi usaha kerajaan, seperti projek MyHIX Malaysia. Objektif utama adalah untuk memperkenalkan idea penyelesaian multi-komponen dan penyebaran untuk HIE berskala besar sebagai pendekatan baru yang berbeza daripada pendekatan pusat yang sedia ada, tetapi tidak menganggu keadaan semasa dan tiada kos setara kepada mana-mana pemegang kepentingan (stakeholders) yang terlibat. Pendekatan yang dicadangkan menyediakan satu rangkakerja yang diedarkan dimana data pesakit dibawa oleh pesakit itu sendiri dalam bentuk Rekod Kesihatan Peribadi mudah alih (mPHRs), biasanya dalam telefon pintar

mereka. Kaedah ini menggunakan konsep mPHR dalam cara yang baru – sebagai unit penyimpanan teragih– dan akan dibandingkan dengan pendekatan pusat semasa yang bertujuan untuk mengumpulkan data pesakit dalam repositori utama dan mengedarkannya melalui enjin pusat. Sistem mPHR individu mampu bersambung secara selamat dengan pelbagai sistem penjagaan kesihatan melalui antaramuka yang sesuai. Antaramuka ini adalah satu aplikasi lain yang dijalankan pada peranti terminal khas (seperti tablet) pada akhir sistem penjagaan kesihatan untuk memastikan kebolehoperasian dengan telefon pintar pesakit. Rekabentuk terperinci dan operasi pendekatan yang dicadangkan telah disediakan dan dipertimbangkan, menghasilkan rangkakerja yang jelas dan multi-komponen untuk HIE. Rangkakerja yang dicadangkan terdiri daripada tiga komponen utama; mPHR disisi pesakit, legasi HIS disisi penyedia penjagaan kesihatan, dan peranti antaramuka diantara keduanya. Keseluruhan rangkakerja disahkan melalui pelaksanaan prototaip menggunakan aplikasi perisian untuk mPHR dan lapisan antaramuka, dan sumber terbuka sistem Rekod Perubatan Elektronik (EMR) untuk mewakili HISs legasi yang digunakan oleh penyedia penjagaan kesihatan. Pelbagai kes pengunaan simulasi dan scenario telah dibentangkan untuk menunjukkan operasi rangkakerja dan kesahan keseluruhannya. Pengesahan rangkakerja yang dicadangkan boleh membawa kepada penyelesaian praktikal terhadap masalah berat HIE yang mengelakkan kos melaksanakan rangkaian global tunggal untuk menyambungkan kesemua sistem penjagaan kesihatan, dan memastikan data yang diperlukan oleh setiap pesakit boleh didapati bila-bila masa dan dimana sahaja ia diperlukan.

Katakunci: pertukaran maklumat kesihatan, bioinfomatik, NFC, pengkomputeran mudah alih, mPHR

ACKNOWLEDGEMENTS

My sincere gratitude goes to all those who supported me through this long journey of Ph.D. First I want to thank my supervisor Professor Dr Miss Laiha Mat Kiah for her patience, guidance and support since the first day I have started my Ph.D. She has never stop believing and supporting me especially in those difficult moments. It has been an honor to be her Ph.D student. I appreciate all her contributions of time, ideas, and funding to make my doctoral experience productive and stimulating.

Besides my supervisor, I would like to thank my co-supervisor Associate Prof. Dr. Rafidah Binti Md Noor for her insightful comments and encouragements.

I would like to appreciate the High Impact Research (HIR) unit, University of Malaya, for providing me the position of Research Assistant (RA) and a partial fee waiver to support my doctoral program.

Throughout this research, I am particularly indebted to Dr. Ahmed Al-Haiqi who helped me to overcome most of the technical difficulties faced during the implementation phase and provided me the full support required for completion of this research.

At last, I would like to thank my entire family members for all their love and friendly encouragements. To my late father who saw the initiation of this process, offering his full support to make it possible. He always wished to call me a Doctor. (I miss you so much). To my mother who raised me with a love of science and supported me in all my pursuits. To my brother and grandmother who always wish me to achieve higher stages throughout my life. And most of all to my loving daughter Sarah, I love you so much my sweetheart, live always happy.

Thank you very much everyone.

Mohamed Shabbir

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

AES	:	Advanced Encryption Standard
AP	:	Access Point
API	:	Application Programming Interface
APK	:	Android Package Kit
BSS	:	Basic Service Set
CIA	:	Confidentiality, Integrity and Availability
CIS	:	Clinic Information System
CPD	:	Continuous Professional Development
CPU	:	Central Processing Unit
CRM	:	Consumer Relation Management
CTI	:	Client-Terminal Interaction
DES	:	Data Encryption Standard
ECC	:	Elliptic Curve Cryptography
EHR	:	Electronic Health Record
EMR	:	Electronic Medical Record
ESS	:	Extended Service Set
GDS	:	Group Data Services
GPL	:	General Public License
GUI	:	Graphical User Interface
HAPI	:	HL7 Application Programming Interface
HIE	:	Health Information Exchange
HIS	:	Hospital Information System
HIPAA	:	Health Insurance Portability and Accountability
HL7	:	Health Level Seven

HRMIS	:	Human Resource Management Information Systems
HTI	:	HIS-Terminal Interaction
IBSS	:	Independent Basic Service Set
IDE	:	Integrated Development Environment
IEC	:	International Electrotechnical Commission
IEEE	:	Institute of Electrical and Electronics Engineers
IHE	:	Integrated Health Enterprise
iOS	:	iPhone Operating System
ISO	:	International Organization for Standardization
JAR	:	Java ARchive
JDK	:	Java Development Kit
LHP	:	Lifetime Health Plan
LHR	:	Lifetime Health Record
LLCP	:	Logical Link Control Protocol
MD	:	Message Digest
MDEC	:	Multimedia Development Corporation
MOH	:	Ministry of Health
MIMOS	:	Malaysian Institute of Microelectronic Systems
mPHR	:	mobile Personal Health Record
MyHIX	:	Malaysian Health Information Exchange
NFC	:	Near Field Communication
NFCIP	:	NFC Interface and Protocol
NHIE	:	Nationwide Health Information Exchange
NIST	:	National Institute of Standards and Technology
NwHIN	:	Nationwide Health Information Network
ONC	:	Office of the National Coordinator

OS	:	Operating System
OSS	:	Open Source Systems
PACS	:	Picture Archiving and Communications System
PAS	:	Patient Administration Systems
PHR	:	Personal Health Records
PHR-S FM	:	Personal Health Record System Functional Model
PID	:	Patient IDentifier
POS	:	Point Of Sale
P2P	:	Peer to Peer
RC	:	Rivest's Cipher or, more informally, Ron's Code
RFID	:	Radio-Frequency Identification
RPC	:	Remote Procedure Call
RSA	:	Rivest-Shamir-Adleman
SHA	:	Secure Hash Algorithm
SMS	:	Short Message Service
SQL	:	Structured Query Language
TC	:	Teleconsultation
TCI	:	Terminal-Client Interaction
THI	:	Terminal-HIS Interaction
UCI	:	User-Client Interaction
URL	:	Uniform Resource Locator
USB	:	Universal Serial Bus
Wi-Fi	:	Wireless Fidelity
WLAN	:	Wireless Local Area Network
WPAN	:	Wireless Personal Area Network
XML	:	eXtensible Markup Language

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

In the first part of the chapter, the necessary background for the research context and motivation is provided, including the concepts of Electronic Medical Record/Electronic Health Record (EMR/EHR), mobile Personal Health Record (mPHR), requirements of secure transmission, and the need for nationwide health information exchange. Next, the problem statement is formulated and justified. After that, the aim of the research is stated, followed by the list of the specific research questions to be addressed in the thesis and the corresponding objectives to be achieved, followed with a discussion on the significance of this research study. The scope of study is determined next and the chapter concludes with a brief outline of the complete thesis.

1.1 Research Background

The main theme in this thesis is to propose a practical solution for the exchange of health information on a nationwide level. As this exchange is bound to be secure, any approach for the problem must consider security aspects in its core design. As such, this work extends over quite few concepts in the healthcare and information technology domains, for which a brief introduction is provided to lay the way for further parts of the thesis.

1.1.1 EMR/EHR Systems

Electronic Medical Record (EMR) / Electronic Health Record (EHR) systems are more than electronic versions of the paper-based records. Those systems are computer-based systems for managing and delivering data required for patient care. The main structure of electronic medical records include demographic elements (e.g. first name, last name, address, city and zip code), visit notes, prescription, allergies, medications, and problems (Evans, 1999). The design of EMR needs to be considered for all medical

professionals because medical services cannot be accomplished by physicians alone, but also requires the involvement of other medical professionals (Li, Zhang, Chu, Suzuki, & Araki, 2012).

EMRs are used through the entire treatment process. It is increasingly noticed that in many hospitals, EMR is the most frequently used system as the core of the hospital management system (Li et al., 2012). To manage an EMR system efficiently, several features must be taken into consideration. For example, electronic medical records need to be stored using proper database management systems for efficient data storage. Proper user interfaces are also required to perform different EMR operations including retrieval of the information from the database. Furthermore, medical data are always in transmission mode; hence proper transmission techniques must be considered while implementing medical record systems.

1.1.2 The Requirement of Secure Transmission

All data transmitted over the Internet or any local network are subject to being attacked (Silverman, 2001). Some of these data could be sensitive information such as credit card numbers, government data or health information. Serious problems may occur if these data are hacked. For example, any unauthorized modification in the patient's record during the transmission time will result in wrong medical prescription by the doctor. Furthermore, information leakage of an ordinary patient may not cause any problem, but if the patient is a prominent government leader or celebrity, leakage of medical data may lead to far-reaching consequences. In addition, an individual's medical records are considered a private asset and therefore are protected by law. Hence, ensuring the secrecy of EMRs is an extremely important task (Chhanabhai & Holt, 2007). This applies equally when the data are at rest or on move for exchange between different healthcare stakeholders.

1.1.3 Nationwide Health Information Exchange (NHIE)

Transmission of health information is required not only to be secured, but also to cross from a healthcare provider to another, possibly over the boundary of the entire country. This led to the introduction of the concept of Nationwide Health Information Exchange (NHIE), and possibly a corresponding healthcare network. A nationwide healthcare network is a web-service based series of specifications designed in some countries to exchange healthcare-related data securely.

The United States, for example, invested 30 billion USD to develop a nationwide healthcare network under the U.S Office of the National Coordinator for Health Information Technology (ONC) for connecting the entire healthcare providers in USA and enabling them to exchange health information whenever needed. It is often abbreviated as the NHIN or NwHIN (Lenert, Sundwall, & Lenert, 2012). A healthcare system participating in the NwHIN acquires connectivity through a 'certified exchange' (to be defined in federal regulation), and such exchange would have licensed connectivity charges and data exchange fees to support their public utility-like functions (Lenert et al., 2012).

The NwHIN approach taken in the USA is proven to be a complex task for government compared to other approaches used in countries like the United Kingdom, Australia and Canada (Lenert et al., 2012). The approach used in the US is integrating nationwide software systems for health data exchange i.e. each hospital is connected with all the hospitals in the region forming a mesh network topology. On the other hand, the approach proposed in the UK is a more centralized option, where government entities have primary responsibility for information exchange and the government leads the implementation of both electronic records systems and health data exchange. The

centralized medical system is based on the cloud technology where all the medical data are stored.

Malaysian journey with eHealth, however, reveals a "top-down" approach led and overseen by the Ministry of Health (MOH). The government initiative started in 1997 with the Telemedicine Blueprint (MOH, 1997). Along the history of MOH to realize this initiative, it went through several stages during which the term was changed into Telehealth (Ghani, 2008). After a few initial projects, MOH took under consideration developing an integration engine that gathers data from different healthcare providers, and a new initiative was commenced in 2008 by MOH with funding from Multimedia Development Corporation (MDEC). The new project is known as the Malaysian Health Information Exchange (MyHIX).

MyHIX is the integration engine in MOH's Integrated Health Enterprise (IHE) framework, implementing the sharing of patient's discharge summary between the facilities of MOH using Hospital Information System (HIS) and Clinic Information System (CIS). Initially, it was implemented at four hospitals as pilot projects, then one more hospital and another clinic joined. The project was appointed later to Malaysia's national R&D center in ICT, MIMOS since 2012 (MIMOS, 2013), and currently is assigned to ViaMED (ViaMED, 2017). In summary, the Malaysian experiment tends to a more centralized approach in which the government, represented by the health ministry (and the Telehealth Division in particular) leads and supervises the implementation of the nationwide health information network.

1.1.4 Mobile Personal Health Records (mPHR)

Current methods used to store and transmit medical data are inefficient for consumers (Kharrazi, Chisholm, VanNasdale, & Thompson, 2012). Traditional health records are normally controlled by individual healthcare providers. End consumers such

as patients can hardly access their data directly. It becomes even more complicated when the medical data of a single patient are residing in different provider databases. Personal Health Records (PHR) stood out as one of the solutions to the increasing demand of patients for flexible access to health information and services (David C Kaelber, Jha, Johnston, Middleton, & Bates, 2008). The requirement of the patients to access their records increases day by day, and every patient is in need of his/her records (Maloney & Wright, 2010).

Complete and accurate health information is important for both patients and physicians. The knowledge about patient's medical history and condition critically informs diagnosis and treatment (Cushman, Froomkin, Cava, Abril, & Goodman, 2010; Maloney & Wright, 2010). On the other hand extra unnecessary charges resulted from redundant diagnostic testing can be reduced by accessing patient records history (Lenert et al., 2012). There is no standard definition for PHR so far; however, PHRs are often described as patient-centered applications on different devices that allow certain parts of patients medical data to be collected, organized and maintained by the individual patient (Kharrazi et al., 2012).

Traditionally, a copy of the patient's PHR was provided to each patient on USB drives, CDs, and other electronic storage devices. However, with introduction of the smartphones and its numerous various applications it became possible for patients to obtain their PHRs on their smartphones. As current technology becomes progressively portable and interactive, smartphone and tablet computers stand out as a new prospective platform for PHRs; hence, the term mobile Personal Health Record (mPHR). One of the driving forces for mPHR is the increased predominance of smartphones and the increased literacy of using them among users (Cruz Zapata, Hernández Niñirola, Idri, Fernández-Alemán, & Toval, 2014; Kharrazi et al., 2012).

1.2 Problem Statement

At the time of patient registration or patient discharge, incomplete or inaccurate data can contribute to making faulty medical decisions, or improper monitoring of patient's condition during follow up care (Kripalani et al., 2007). On the other hand, a complete medical history of the patient may save the patient's life and improve patient outcomes (Hargreaves, 2010; Lupse, Vida, & Stoicu-Tivadar, 2012; McHome, Sachdeva, & Bhalla, 2010). It is empirical to have patients' data readily available in the right format whenever and wherever needed. Because patients' data are usually fragmented across the systems of several providers, it is crucial to enable the exchange of patients' health information among those providers.

Several challenges face nationwide health information exchange (NHIE), within and beyond technology. From a technical perspective, the goal of NHIE involves fully interoperable, patient-centered, and easy-to-use systems, as pointed out in (Kellermann & Jones, 2013). Interoperability can only be ensured if various healthcare providers use homogeneous technologies across their legacy systems at both the syntactic and semantic levels, which is very unlikely for various reasons, one of which is the differences in the historical development of those systems. A more viable approach to achieve interoperability is using common languages or protocols for seamless interaction and communication. At present, relying on common protocols is the only feasible approach and the target for standardization efforts. Standards do exist at the data level, such as the HL7 set of standards (HL7, 2017a). At the level of software systems, additional support is necessary for the data standards to intercommunicate. Owing to the great variety and volume of healthcare providers and their corresponding systems and policies, convincing everyone to add the required support proved to be challenging enough even for government authorities.

Interoperability is only one side of the HIE equation, which is encountered at the point of exchange. The other side of the equation is the transmission of information to the points of exchange. To enable HIE, a model for interconnectivity is needed. At the national level, current solutions for patient information exchange are mainly in the form of governmental initiatives, which normally take two forms. The first approach is by forming a nationwide network for point-to-point data exchange with the aid of standards and interoperability protocols. The other approach is based on the utilization of centralized servers, where sets of patient information are collected by central repositories and circulated via different levels of centralized engines. This approach might use several interconnected servers in the form of an electronic cloud to manage the exchange of medical information between healthcare providers who are connected to the cloud. The administrative and implementation costs of both approaches are very high, and they have proven difficult to adopt and deploy on a large scale.

Both approaches also suffer from several obstructions and challenges, including non-compliance to standards and concerns on integration, interoperability, privacy, and usability. For many years, these barriers have hindered governments in many countries from fully implementing HIEs, including Malaysia. This thesis is motivated and driven on this basis. The main purpose of this work is to introduce a new approach for HIE, which works around the problems of the more central approaches, while still ensuring a secure exchange of medical data. In particular, this work envisions a more distributed model, in which patient data are carried by the patients themselves in the form of personal health records, typically on their mobile handheld devices. A distributed model for health information exchange would comprise several components, including the introduced mPHR systems and the traditional EMR systems, besides any other necessary parts to interconnect those components together. Hence, the work in this

thesis is to seek the design and development of a complete, end-to-end and coherent framework for solving the hard problem of NHIE.

1.3 Research Aim

The aim of this research is to propose an alternative or complementary approach for government-centered projects for the Nationwide Health Information Exchange (NHIE). The proposed framework is aimed to be practical, cost-efficient, and readily deployable, by innovatively using the available technologies, and requiring no changes to the current infrastructure or functional systems. The framework is aimed to comprise several systems and related methods. The basic idea is that patient health information is carried by the patients themselves in the form of mPHR systems.

1.4 Research Questions (RQs)

Based on the discussion presented above, the following research questions are formulated to set the direction of this research:

i. What is the current situation of the nationwide HIE in Malaysia?
ii. What are the main requirements for a successful HIE nationwide?
iii. Is there an alternative approach to centralized data exchange?
iv. What are the requirements for building a secure mPHR system?
v. What are the requirements for building a secure interface between systems?
vi. How to solve the problem of interoperability between mPHR and EMR systems?
vii. How to solve the problem of interconnectivity between mPHR and EMR systems?
viii. How can the proposed solution be realized using available technology?
ix. How to validate the implementation choices of the proposed design?

Research questions are devised to keep the research in line with the objectives. Table 1.1 shows the relationship between the research objectives and the research questions.

Table 1.1: The link between objectives and research question

Objectives	Research Questions
a) To identify the current situation of nationwide health information exchange in Malaysia, and the requirements for solutions to implement secure and seamless exchange of health data between healthcare providers.	i. What is the current situation of the nationwide HIE in Malaysia? ii. What are the main requirements for a successful HIE nationwide?
b) To propose a novel framework for nationwide HIE utilizing mPHRs and custom terminals at HIS points. The proposal should outline the overall architecture of the framework as well as the detailed design of individual components and their operation.	iii. Is there an alternative approach to centralized data exchange? iv. What are the requirements for building a secure mPHR system? v. What are the requirements for building a secure interface between systems? vi. How to solve the problem of interoperability between mPHR and EMR systems? vii. How to solve the problem of interconnectivity between mPHR and EMR systems?
c) To implement a prototype version of the proposed framework with the help of the current tools and technologies in order to prove the concept of the solution.	viii. How can the proposed solution be realized using available technology?
d) To validate the prototype version of the proposed framework based on a set of test cases generated from a simulated case study.	ix. How to validate the implementation choices of the proposed design?

1.5 Research Objectives

The objectives of this research are as follows:

a) To identify the current situation of nationwide health information exchange in Malaysia, and the requirements for solutions to implement secure and seamless exchange of health data between healthcare providers.

b) To propose a novel framework for NHIE utilizing mPHRs and custom terminals at HIS points. The proposal should outline the overall architecture of the framework as well as the detailed design of individual components and their operation.

c) To implement a prototype version of the proposed framework with the help of the current tools and technologies in order to prove the concept of the solution.

d) To validate the prototype version of the proposed framework based on a set of test cases generated from a simulated case study.

1.6 Significance of Study

Health information exchange is one pillar for transforming the Malaysian health system into the digital economy agenda. As national attempts to achieve this goal has not (yet) seen the anticipated success, approaches of more practical even though ad hoc nature can serve as a transient solutions that might prove itself resilient enough to last for longer times and even impose itself as a de facto reality, especially if endorsed by the proper sponsors.

The resulting framework out of this thesis can be adopted and utilized by interested parties as long as there is no effective mechanism to exchange data between healthcare centers. The estimated life span of an operational and potentially commercialized version of the framework can run to several years. Stakeholders in the healthcare industry would have special interest in the idea as a practical and economical approach to achieve the long sought effective exchange of patients' health information. Those stakeholders include individual care providers, large public hospitals as well as smaller private clinics and health centers. However, government health agencies will particularly have a special interest in the idea, as governments are increasingly concerned about the problem of nationwide health information exchange. This study furthermore contributes to healthcare informatics literature, pertaining to nationwide HIE in general.

1.7 Scope of Study

The ideas for information transmission and exchange among different distributed components nationwide are developed in this thesis for the particular application of healthcare information. The techniques and standards involved are devised and selected based on the norm in healthcare industry. The research in this work is probably not applicable to electronic transmission of data in other areas such as banking and finance. Security has been integrated in the design of the proposed solution as a key non-functional requirement, though other requirements such as usability have received less attention in the design of the various apps that compromise the proposed solution. Adherence to standards has also been regarded as a key factor, as well as cost efficiency.

1.8 Thesis Layout

The remaining parts of this thesis are organized as follows. Chapter 1 sets the stage for the rest of the thesis. It introduces the motivation behind the whole work, defines the problem statement, and derives the research questions. The chapter also sets the objectives to be achieved and maps those objectives to the posed research questions. The significance of research is discussed and its scope is described.

Chapter 2 presents a complete review on health information systems (HIS) and the process of health information exchange among health providers. This chapter also provides a background on existing approaches for nationwide HIE, the concept of mobile PHR and a few enabler technologies for the solution introduced in this thesis. Finally, previous studies are summarized based on the mechanisms of exchanging EHRs as well as the security concerns.

Chapter 3 explains the general methodology used throughout this research in order to achieve the objectives. The whole structure of this research along with its different phases are depicted in a single figure, and the main phases are described accordingly.

Chapter 4 presents the design of the proposed framework and describes its structure and related components in detail.

Chapter 5 discusses the realization of the proposed framework in a prototypic implementation. The aim of this chapter is to prove the concept of the proposed framework. The process of implementing the different components of the proposed framework is explained in detail.

Chapter 6 focuses on testing and validating the proposed and implemented framework in order to show whether it satisfies the specified requirements. A validation scenario is described and then various points related to the framework design and implementation are discussed.

Chapter 7 provides an overall summary of the research and the significance of its findings. This chapter highlights the objectives that had been achieved followed by research limitations, and its significance and contributions. Suggestions on further possible improvements to the framework are also provided.

CHAPTER 2: LITERATURE REVIEW

As per the earlier discussion in chapter 1 and its subsequent sections, a detailed literature review has been conducted on all the interacting components of the proposed framework. Adoption of an Electronic Health Records (EHRs) systems requires adopting several existing standards and protocols with regard to their security and transmission process. This chapter will discuss and focus on all the interacting components of EHRs as well as the involved standards and protocols in Health Information Systems (HIS). Comparison tables are brought out from the previous studies based on the mechanisms of exchanging EHRs as well as the security concerns.

2.1 Health Information Systems

Any system has the ability of capturing, storing, managing and transmitting individual's health records within a healthcare sector is often referred as Health Information System (HIS). From the literature the definition of health information systems has different views, for example some articles focuses on the organizational aspects of information processing and other articles focusses on the technology used (Chou, 2011). HIS includes disease surveillance systems, laboratory information systems, hospital patient administration systems (PAS) and human resource management information systems (HRMIS). Nearly all people working in healthcare organization has a massive demand for information which needs to be accomplished in order to achieve high quality and efficient patient care.

The quality of information processing is important for the competitiveness of a hospital and that is because nearly all areas of the healthcare organization depend on it. In case if HIS are not managed and operated systematically they tend to develop disordered information which in turn leads to negative consequences such as low data

quality which results in low quality of patient's care. On the other hand, systematic information management contributes in preventing such HIS failures which results in high quality and efficient patient care. Overall, a well-functioning HIS is an integrated effort of different sectors of a healthcare provider.

Electronic Medical Records (EMR) / Electronic Health Records (EHR) are more than an electronic version of the paper-based record. It is a computer based generated data for managing and delivering data required for patient care. Although the two terms looks identical, however there is a difference in the concept of the both terms. According to Garets and Davis (2006) EMR is composition of clinical data repository, clinical decision support, controlled medical vocabulary, order entry, computerized provider order entry, pharmacy, and clinical documentation applications. These records are used by healthcare practitioners to document, monitor, and manage health care delivery within a care delivery organization (CDO) and the data in the EMR are owned by the CDO. On the other hand EHR is a subset of CDO and it is owned by the patient. The main structure of electronic medical records include demographic elements (i.e. first name, last name, address, city and zip code), visit notes, (a specific number of characters in the database are reserved for each patient thus allowing the doctor to write his prescription), allergies, medications, and problems (Evans, 1999). The design of EMR needs to be considered for all medical professionals because medical services cannot be accomplished by physicians alone, but also requires the involvement of other medical professionals (Li et al., 2012).

Nowadays in any hospital EMR system is the most frequently used system because it is the core of the hospital management system and it is used throughout the entire treatment process (Li et al., 2012). To manage an EMR system efficiently the following features must be taken under consideration. Data storage: Proper database management

system need to be involved in storing the electronic medical records for example Oracle. Data retrieval: Proper user interfaces are required to perform different EMR operations including retrieval the information from the databases. Data Transmission: medical data are always in transmission mode. Hence, proper transmission techniques must be considered while implementing medical systems. Security aspects must be applied on data while transmission. Integration has to achieve between the source and destination. In United States, the use of EHR technology is already widely adopted. It is estimated that 55% of medical professionals are using EHR platforms (Silva, Rodrigues, de la Torre Díez, López-Coronado, & Saleem, 2015).

2.2 Health Information Exchange (HIE)

The process of interchanging healthcare information electronically across organizations within a region, community or hospital system is known as HIE (Vest & Gamm, 2010). HIE enhances the moving of electronic data among scattered clinical health care systems while protecting the meaning of the information being exchanged. The main purpose of HIE is to facilitate access and retrieval of medical data. HIE allows efficient patient management, better coordinated heath care, and assessing up-to-date patient information. There are several advantages that can be obtained by the patients as well as the healthcare centers when the health information is exchanged. From the patient perspective, it improves payment coordination, clinical outcomes, transition of care, visit experience and satisfaction. It also reduces or even eliminates duplicative or unnecessary procedures or tests. From the healthcare perspective, it reduces healthcare costs, improves monitoring of patient movement and disease management and finally it improves patient satisfaction and provider experience.

Beyond the adoption of electronic health records in the medical domain, nations now, more than ever, look forward to reaping the full potential of digitizing patients'

records and computerizing the medical care process. That is, an instant access to health information in the right place at the right time and in a usable format. This goal involves, as pointed out in (Kellermann & Jones, 2013), fully interoperable, patient-centered, and easy- to-use systems.

According to Northrop et al. (2006) the term interoperability refers to the ability of two or more systems or elements to exchange information and to use the information that have been exchanged. Brailer (2005) defined interoperability as the ability to exchange health information, and thus realize the societal benefits promised by the adoption of EHRs. Interoperability can be divided into technical and semantic. Technical interoperability allows data to be moved from one system to another independently of the domain or the meaning of what is being exchanged. Semantic interoperability, on the other hand, obtains the meaning of the data then allows computers to share, understand, interpret, and use the data without ambiguity.

To exchange information, there is the obvious requirement of transmitting data via some networking technology, in addition to the critical role of developing and promoting health standards (Kuperman et al., 2010). Substantial net value can be obtained if HIE could be fully implemented (Walker et al., 2005). HIE has received a lot of attention in both academic research as well as governmental initiatives. A good source for the history of early efforts in HIE up to late 2010 is (Kuperman, 2011). Regardless of the model of exchange, the concept of sharing patient data with several entities always brings the concerns of patient privacy and security.

2.2.1 Benefits of HIE

According to previous studies, the clinical benefits of electronic data exchange would be substantial and that financial benefits would outweigh costs (Hillestad et al., 2005; Sprivulis et al., 2007; Walker et al., 2005). Healthcare costs could be reduced if

duplicate tests were eliminated. Duplicating tests could result from ignorance of examination results performed elsewhere or from incentive of fee-for-service payment (Payne, Detmer, Wyatt, & Buchan, 2011). In the special case of back pain emergency evaluation, for example, the use of health information exchange is associated with 64% lower odds of repeated diagnostic imaging, as indicated in (Bailey et al., 2013). Rather than cost reduction, there are other benefits of HIE discussed below in brief.

(a) ***Safety***

Healthcare is likely to be safer if information such as allergies and current medications are known when new treatments are ordered (Payne et al., 2011). Emergency care in particular can be safer if health information were exchanged (Shapiro et al., 2006). According to David C. Kaelber and Bates (2007), up to 18% of the patient safety errors generally and as many as 70% of adverse drug events could be eliminated if the right information about the right patient is available at the right time. HIE can make this possible.

(b) ***Time Saving***

Time can be saved if a consultant or emergency room physician can verify information from the primary care provider's record rather than gathering it a new (Payne et al., 2011). Saving time in this manner might also imply saving a lot of patients' frustration and inconvenience, up to saving their lives, when timely critical response is a must. This advantage is applicable for history information in particular, and in case of recent diagnosis.

(c) ***Assessing quality of care***

Use of administrative data in assessing healthcare quality has been suggested early on (Iezzoni, 1997). Currently, administrative functions are more mature, and the accuracy and completeness of administrative data are better than ever. Sharing of

administrative data follows the question of who will make use of those data. Whether government would give a "window" into the data to third party entities, or restrict the access to them will decide upon the exchange model for such data and whether that lies under the umbrella of HIE.

(d) ***Research resource***

A natural byproduct of available clinical and administrative data is an increasing source of datasets (Safran et al., 2007). Datasets are the fuel for research in many disciplines, and many researchers have discussed the use of the large databases of aggregate medical data in health information networks for research. Combined with data mining and statistical analysis tools, these repositories of health information can produce great advances in medical knowledge as well as healthcare quality and better strategic management. Digital tracking of health information makes it easier to observe trends in the general population and track successful (and less-successful, for that matter) treatment methods (Benli, Yaylacicegi, Vetter, Reinicke, & Mitchell, 2012). The authors in (M. Song, Liu, Abromitis, & Schleyer, 2013) reviews the current status of reusing electronic patient records for dental research. Use of routinely collected EMR for pediatric clinical research is inspected in (Wasserman, 2011), where it is noted that one barrier to this use is the fact that pediatric health data are collected for the purpose of clinical documentation and billing rather than research. This gives rise to issues like accuracy, completeness, compatibility between settings, and ease of extraction. In fact these issues apply to medical records in different healthcare fields. Safran et al. (2007) discuss the secondary use of health data, applying personal health information for uses outside of direct healthcare delivery. It includes activities like analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing and other business applications. It is worthy to notice that data mining in the medical domain is unique. The authors in (Cios & William Moore, 2002) emphasize

this uniqueness in medical data mining as medicine is primarily directed at patient care, and only secondarily as a research resource, and researchers from other fields might not be aware of the special constraints associated with privacy-sensitive, heterogeneous, but voluminous data of medicine. Nevertheless, medical data mining, as the authors note, can also be the most rewarding. Finally, it is crucial to consider that the aforementioned benefits in many cases are subject to the moral justification for using personal data without informed consent (Regidor, 2004).

(e) ***Organizational benefits***

HIE is also associated with overall organizational gains, as hospitals that have implemented HIE are associated with higher patient satisfaction (Vest, 2012).

2.2.2 Patient's perception

It is also important to take patients perception on sharing their health data into account. In a pilot program in South Korea to study patients' perception of HIE (Park et al., 2013), the authors reported that despite the concern of patients about information safety and security, respondents in all surveyed groups indicated an acceptance of and willingness to endorse HIE technology. The major factor of the positive support was their perceived benefit of convenience out of eliminating redundant procedures, rather than perceived improvement in quality or savings in costs.

2.2.3 Security and privacy

Healthcare organizations are increasingly becoming under attack by cyber criminals. According to a report by Trustwave, 91% of the technical people they contacted in the sector believe criminals are increasingly targeting healthcare organizations (Elsevier, 2015). However, it becomes worst by failing to implement strong security and poor compliance with best privacy practice. According to the report, more than a third of health organizations conduct vulnerability testing only once a year in addition 35% of

technical people mentioned that their organizations does not have enough dedicated security staff. However, around 10% only of the health organizations' IT budgets goes towards cyber-security and protecting patient's information (Elsevier, 2015).

Another report produced by Symantec mentioned that the healthcare industry accounted for 36% of all security incident breaches in 2013. At 44%, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industries in 2014 (He & Johnson, 2015). With increasing number of such incidents, health organizations may lose their reputation, customer confidence, productivity and it may lead to direct financial losses. Hence, security and privacy of patients in healthcare are among major areas of concern. In this regard, the authentication and authorization when data are being exchanged as well as end-to-end data protection are critical requirements as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented (Moosavi et al., 2016).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes costly penalties on healthcare organizations for noncompliance with its privacy and security rules (Harvey & Harvey, 2014). Privacy and security legislation enforces any security architecture for health platforms to support several privacy and security principles, including confidentiality, integrity, and availability. Confidentiality ensures that unauthorized parties should not access to data while its being transmitted or stored; integrity ensures that there are no intentional or accidental changes to transmitted and stored data; and availability ensures accessibility of resources or assets at any time regardless of location.

Patient health information is of high sensitivity from a privacy perspective, thus confidentiality is a major concern in any healthcare records system. Securing the integrity of medical records is perhaps more important, as the life of the patient might

depend on the correctness of the health information. Likewise, availability of health data when needed is at the heart of the whole idea of health information exchange. Accountability and access control are two important measures to authorize and audit access to medical records.

All these requirements are essential in any electronic health system, and become more persisting when data are brought outside their origins and shared with external parties. Allowing the users to access information from virtually anywhere, essentially expands the universe of ineligible intruders, thus severely complicating the design and implementation of a secure system (Gritzalis & Lambrinoudakis, 2004). Extensive research has been conducted on the security issues arising from health information exchange. Secure exchange solutions, and security architectures and models for interconnected and distributed health information systems have been suggested by many researchers (Flores, 2010; Gritzalis & Lambrinoudakis, 2004; Liang et al., 2008; Sucurovic, 2007; van der Linden, Kalra, Hasman, & Talmon, 2009). More recently, few researchers also attempted to tailor specific security frameworks in the context of the nascent nationwide health information networking initiatives, such as the US initiative (Benli et al., 2012), or suggest novel solution frameworks to meet challenges of electronic health interconnected infrastructure (W. Liu, Park, & Krieger, 2012).

2.2.4 Standardization Efforts

Healthcare delivery environments are under constant pressure to rationalize the cost of care provisioning while at the same time having to preserve or even increase the quality of care pathways and clinical processes (Blazona & Koncar, 2007). The everyday workflow in several healthcare providers has entered certain degree of independence. The cause of this independency may be due to the difficulty in interoperability between information systems. This difficulty can be overcome through

the implementation and adoption of standards (Barbarito et al., 2012). Recently several healthcare standards has been introduced for various purposes. Example of such standard is HL7. Health Level Seven (HL7) is an international interoperability standard for healthcare oriented communication protocol at the seventh layer of the OSI communication model i.e. the application layer (Miranda et al., 2012).

In the medical context HL7 standard is identified as the world's leading medical ICT standard that is envisioned to provide the umbrella for medical data interoperability (Blazona & Koncar, 2007). HL7 provides a framework for the exchange, integration, sharing, and retrieval of electronic health information (EHR). HL7 concentrates on the syntax of what is exchanged, rather than the technology or mean by which this communication occurs nor the underlying architecture (Miranda et al., 2012). Basically HL7 is not a programming language; it works using interfaces, which is also referred as HL7 interface engine. HL7 Interface engine is software which works as a go-between for different systems. This software monitors different type of interfaces and communication points and performs actions according to the rules defined by the HL7 organization standard.

Today the HL7 standard represents the foundation of many healthcare information management systems. It provides structures and mechanisms for data communication between administrative and clinical data without focusing on a specific healthcare domain or communication technology. The version 3 of HL7 standard focuses on the methodology how do the clinical and ICT experts specify the final data sets that are exchanged between systems, and does so by founding all its' artifacts on HL7 Reference Information Model (Blazona & Koncar, 2007).

HL7 Message structure

HL7 is comprised of messages that contain segments. Segments contain components and components contain the actual data. There are also subcomponents which further breaks down the data. Components are separated by pipes which has two purposes:

a. Informs the interface how to parse out the data so that it can be transmitted and inserted into databases of another programs.
b. It provides a way to easily read the messages.

Consider the following HL7 message example of ADT (Admission, Discharge, and Transfer) message in Figure 2.1.

```
MSH|^~\&|EPICADT|DH|LABADT|DH|201301011226||ADT^A01|HL7MSG00001|P|2.3|
EVN|A01|201301011223||
PID|||MRN12345^5^M11||APPLESEED^JOHN^A^III||19710101|M||C|1 CATALYZE
STREET^^MADISON^WI^53005-1020|GL|(414)379-1212|(414)271-
3434||S||MRN12345001^2^M10|123456789|987654^NC|
NK1|1|APPLESEED^BARBARA^J|WIFE||||||NK^NEXT OF KIN
PV1|1|I|2000^2012^01||||004777^GOOD^SIDNEY^J.|||SUR||||ADM|A0|
```

Figure 2.1: HL7 ADT message segment

As seen in the above example, the HL7 message contains of segments headers which are three letters abbreviation that defines which kind of data contains in the given segment. For example the first header segment is MSH (Message header) segment which defines things like:-

a. What kind of message it is.
b. When it was sent.
c. What kind of system is sending it?

A concept called counting pipes is used to identify the components. For example in MSH header the components are counted in the header segment referred as MSH;1, MSH;2 and so on. Encoding characters tells the receiving system message type i.e. the type of interface. In the ADT interface message as seen above, ADT^A01 is referred to Inpatient admission. Similarly, there are list of possible events. For example, ADT^A03 refers to inpatient discharge, ADT^A17 refers to bed swap and so on. Considering the second header segment, PID (Patient ID) contains all the information about the patient. Referring to Figure 2.2 the ADT message PID:5.1 APPLESEED and PID:5.2 JOHN.

```
PID| | |MRN12345^5^M11| |APPLESEED^JOHN^A^III| |19710101|M| |C|1 CATALYZE
STREET^^MADISON^WI^53005-1020|GL|(414)379-1212|(414)271-3434| |S|
|MRN12345001^2^M10|123456789|987654^NC|
```

Figure 2.2: HL7 segment for Patient ID

2.3 Nationwide Health Information Exchange (NHIE)

Nationwide healthcare network is web-services based series of specifications designed to securely exchange healthcare related data. It is a 30 Billion USD investment being developed under U.S. Office of the National Coordinator for Health Information Technology (ONC). Nationwide health Information Network is often abbreviated as NHIN or NwHIN (Kuperman, 2011; Kuperman et al., 2010). As the requirement of the patient to access to his record increases day by day, this implies that every patient is in need of his/her records. Systematic health record plays spirited role in the field of delivering appropriate health services to the patient. A healthcare system participating in the NwHIN acquires connectivity through a 'certified exchange' (to be defined in federal regulation). Such exchanges would have licensed connectivity charges and data exchange fees to support their public utility-like functions (Kuperman, 2011).

2.3.1 General Approaches towards NHIE

To enable health information exchange nationwide, a model of interconnectivity is needed. Given the non-functional requirements of security, privacy and interoperability, and the non-technical issues of data ownership and business competition, several approaches could be followed to achieve the goal of NHIE.

One possible approach is to form a nationwide network of point-to-point information exchange through standards and interoperability protocols. Another approach is based on centralized servers, and the collection of patient's data in central repositories and circulating them via some sort of central engine. The latter approach uses several interconnected servers in the form of cloud to centrally manage and exchange the medical data between healthcare providers connected to these servers. The cost of implementation for these approaches is very high. Additionally, yearly charges might be applied to each healthcare provider that participates in the exchange. Both approaches proved hard to widely adopt and deploy, and suffer from several barriers including compliance to standards, integration, interoperability and privacy concerns. These obstacles had set back the government initiatives for nationwide health information exchange for many years in various countries, including Malaysia (Mat Som, Norali, & Ali, 2010).

In England, the national strategy was a top-down approach, organized through a central implementation agency in order to deliver standardized EHR applications. As a result, local organizations were to adhere to the national program rather than implementing their own solutions for EHRs. However, the diversity of stakeholders and variations in the functionalities due to the huge scale of England-wide deployments contributed to deployment delays and to more localized approaches emerging. Over the time the implementation approaches changed, and the top-down, centrally driven

implementation of EHRs has been evolving into more localized solutions (Morrison, Robertson, Cresswell, Crowe, & Sheikh, 2011).

Similarly, Australia approached the top-down strategy through MediConnect program. This program had been intended to provide an Australia-wide, secure electronic system for medication management. Later, MediConnect was incorporated into another program called HealthConnect. HealthConnect was conceived as a national change management strategy, and was to include a move from paper-based records to standardized, digital patient records held at the point of care (Morrison et al., 2011). Figure 2.3 depicts the idea of the centralized approach adopted in several countries including England and Australia.

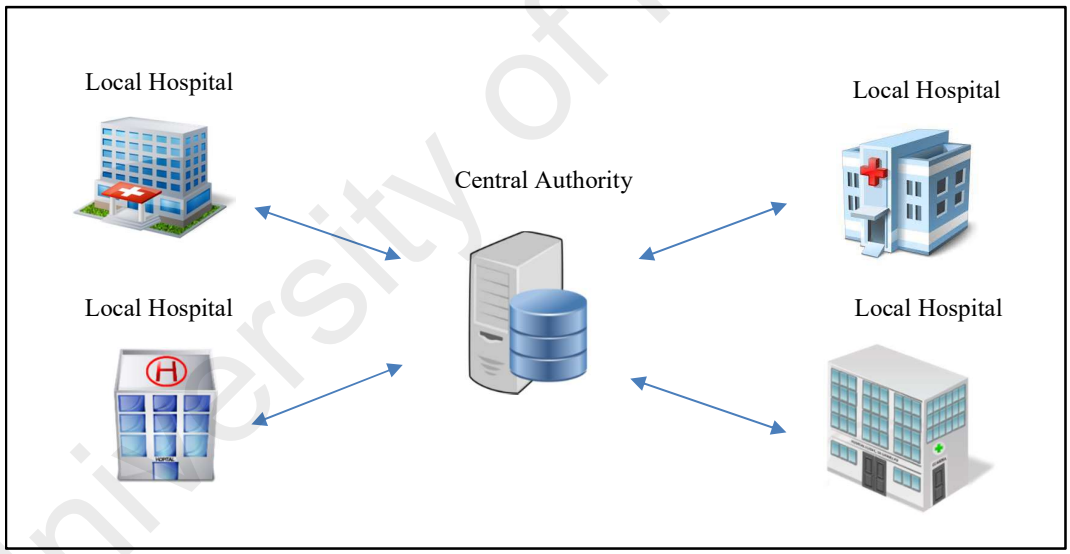


Figure 2.3: Central Approach

In the USA, proponents of this kind of a network noted that it should not contain a centralized government database of personal health information but rather should help to connect existing sources of distributed electronic health data in the framework of a secure network (Shapiro et al., 2006). This approach has been called a 'bottom up' strategy, also referred to as 'federated approach' in contrast to the 'top down'

centralized strategy used in UK (Coiera, 2009; Lenert et al., 2012). Figure 2.4 depicts the idea of federated approach adopted in the United States.

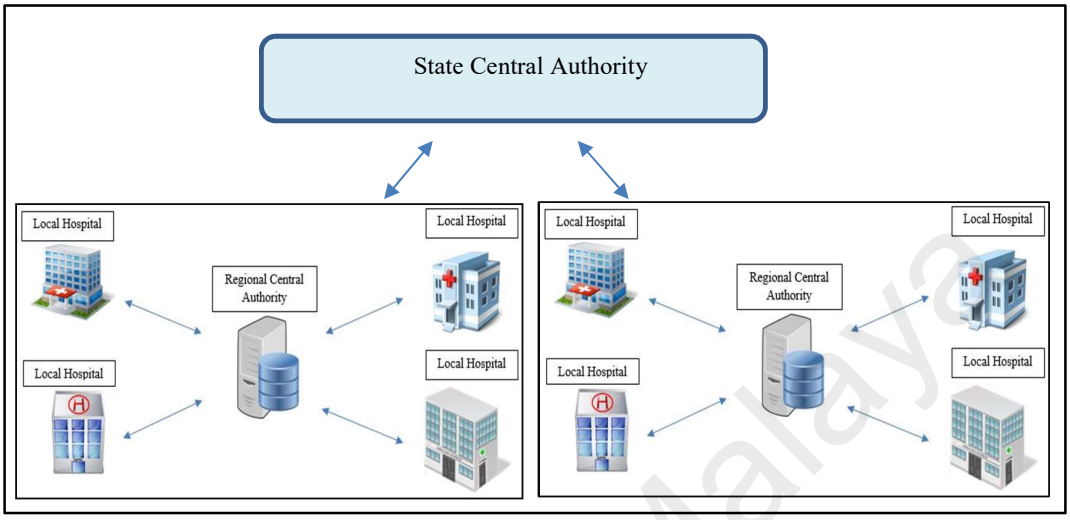


Figure 2.4: Federated Approach

The federated HIE approach consists of several clinical data repositories which are located remotely. Unique patient identifiers are provided to the regional central authority or to the state central authority, and then stored in the state-wide HIE's patient registry, or record locator service. Hence, unlike centralized HIE, in federated HIE patient data are not stored in a centralized accessible location. Patient information continues to be stored locally within the regional central authority. In case of patient data request, a member hospital sends query messages to the HIE's patient registry which in turn contains a "virtual roadmap" of where patient health records are located. When a record is located in the registry, the state central authority transmits the record's physical location back to the requesting hospital. The requesting hospital then must request the patient information from the facility where it is located. The facility storing the information can transmit the data to the requesting hospital through any secure connection.

This approach is considered less interoperable compare to the centralized HIE because it does not allow a simple exchange of information between facilities' EHR systems. The central record locator service is always needed to keep track of numerous duplicate health records at multiple remote locations, which increases the complexity of locating a complete patient's health history and determining which information is the most up to date.

2.3.2 The Malaysian Telehealth Approach

A quick look at the Malaysian journey with e-Health reveals a "top-down" approach lead and overseen by the Ministry of Health (MOH). The government initiative started in 1997 with Telemedicine Blueprint (MOH, 1997). Along the history of MOH to realize this initiative, it went through several stages during which the term was changed into Telehealth (Ghani, 2008). The aim was to establish a flagship project encompassing all services that can be provided via multimedia networks and a range of network-based information technologies for the use of stakeholders to access, manage or deliver healthcare. As stated in the initial blueprint "Information and other services will become more virtual, more distributed, resulting in better, more timely and more efficient healthcare delivery." Virtual in the sense that it does not require physical presence of the patient and/or the physician. And distributed in the sense that it is accessible anywhere needed. MOH restructured the Malaysian Telehealth several times to reflect the evolving needs and gained experience (Som, Norali, & Ali, 2010).

In 2000, a special unit under the ministry was established to take charge of implementing the telehealth flagship project. This unit, named Telehealth Division to mirror its purpose, had setup several pilot projects, some of which targeted the healthcare professionals, including continuing medical education and teleconsultation, while others aimed at providing personalized continual care as well as high-quality

health information for individuals. As indicated in (Allaudin, 2013), the projects cover all aspects of healthcare service delivery, including: Lifetime Health Record (LHR), Lifetime Health Plan (LHP), Group Data Services (GDS), Health Online (MyHEALTH Portal), Continuous Professional Development (CPD), Teleconsultation (TC), and Consumer Relation management (CRM). The LHR project is a cornerstone project in the context of a continuous care delivery. These records are collections of health information on an individual patient that captures data from the patient himself/herself as well as his/her healthcare provider, to be used by all caregivers from birth to death (Hisan, 2012).

Figure 2.5 shows the relative positions of those projects in Malaysia Health ICT Framework (Hisan, 2012). The lower layer, operational layer, corresponds more to EMRs. In the collaborative layer, components found that resemble EHRs, centrally stored in data repositories, where integration (collaboration) between different stakeholders happens. In this layer, the Data Warehouse component is a typical place to perform data mining techniques for research purposes. The upmost layer is the consumer layer, where the government provides specific "windows" into the central databases for the public, including patients and healthcare professionals. Mostly implemented as web portals.

The operational layer include Hospital Information Systems (HIS)s and Clinic Information Systems (CIS)s being deployed in hospitals and clinics, respectively. Deployment of the first such systems made the crucial function of interoperability obvious, where MOH assigned building the applications to several vendors, and their integration was a problem.

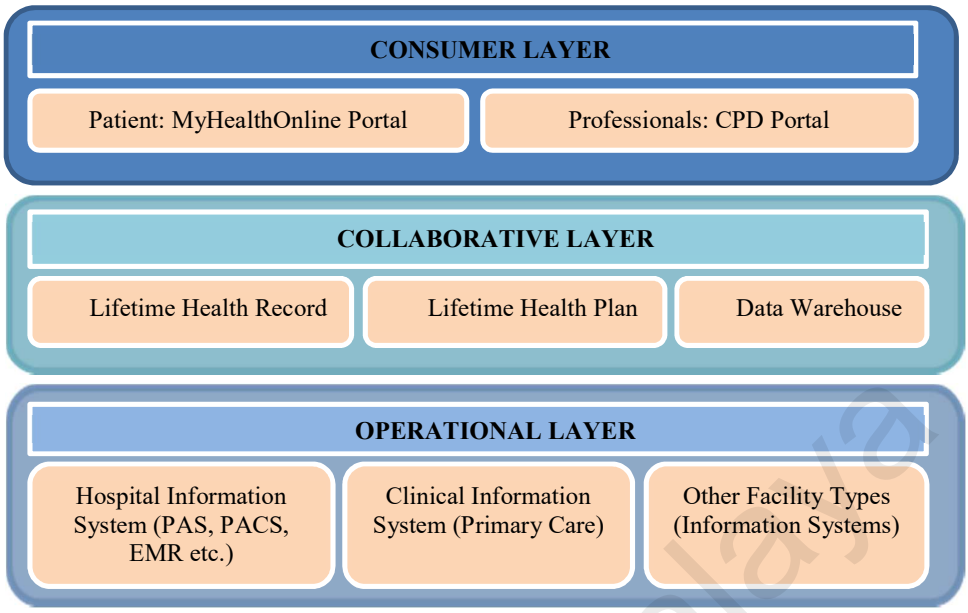


Figure 2.5: Malaysia Health ICT Framework (Hisan, 2012)

In 2007, MOH introduced the Integrated Health Enterprise (IHE) framework. This framework, in turn, introduced "Connectathon": a (CONNECTivity marATHON) jointly organized by MSC Malaysia and the Ministry of Health, during which the vendors or healthcare service providers that have developed data sharing solutions test the compliance of their offerings based on HL7 standard, in a realistic and live interoperability environment (Som et al., 2010).

To realize integration, there exist several requisites: standards for data, messages, documents and workflows (Hisan, 2012). Further, to implement central repositories, a central engine for integration is important. Data and message international standards were adopted (e.g. ICD 10, MDC and DIC for data, and HLZ and CDA for message formats). As an initial proof-of-concept document standard for LHRs, it was decided that discharge summaries would play that role. Discharge summaries are minimal records of physical examination, previous history, laboratory investigation, diagnosis and treatment of the patient to ensure continuous delivery of healthcare. In this way,

LHRs corresponds to definition of EHRs, and depend on the HIS and CIS applications, which are associated with EMRs.

Considering the importance of developing an integration engine and the previous difficulties in implementation, a new initiative was commenced in 2008 by MOH with funding from Multimedia Development Corporation (MDEC). The new project is known as the Malaysian Health Information Exchange (MyHIX). MyHIX is the integration engine in the IHE framework implementing the sharing of patient's discharge summary between the facilities of Ministry of Health using HIS and CIS application systems. Initially, it was implemented at four hospitals as pilot projects, then one more hospital and another clinic joined. In 2012, the development and implementation of MyHIX was delegated initially to the National R&D Centre in ICT i.e., MIMOS (MIMOS, 2013). At present, another group, ViaMED (ViaMED, 2017), is the appointed vendor of the MyHIX project.

Despite the initiatives and efforts made at the topmost levels, the Malaysian approach on NHIE was often met with long delays. To finish the story, MyHIX has now reached version 2.0; however, its implementation is very limited because only 7 of 142 registered hospitals under the MOH participated in the pilot government project (75% of which still employ manual information systems) (Allaudin, 2013). In the most recent Malaysia Telehealth Connectathon held on June 15, 2016 (the fourth since 2008), only three vendors participated and tested their products according to profile specification. The products of these vendors are currently used by MOH hospitals, where MyHIX serves as the integration engine (AeHIN, 2016).

In summary, the Malaysian experiment tends to a more centralized approach in which the government, represented by the health ministry (and the Telehealth Division in particular) leads and supervises the implementation of the nationwide health

information network. Apart from the merits or demerits of such strategy, a compliant architecture is considered when devising a security framework.

2.4 mobile Personal Health Record (mPHR)

There are number of definitions for the term PHR. The easiest way to understand this term, PHR is an electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment (Tang, Ash, Bates, Overhage, & Sands, 2006). As technology becomes increasingly portable and interactive, cellular phones and tablet computers have emerged as a new potential platform for PHRs. Personal Health Records (PHRs) which are based on mobile phones mostly smartphones are referred as mobile PHR abbreviated as mPHR. The integration of PHRs are likely to become fully implemented into patients daily activities with the wide growing and adoption of smartphones by people of all ages and the availability of mobile based PHR applications. To maximize the benefits of this integration, PHRs will need to be continually improved with features that are most useful to patients (Tom, Chen, & Zhou, 2014).

Traditionally, mobile PHRs included USB drives, CDs, and other electronic storage devices that were incorporated into bracelets or wallet cards. The basic function of these portable devices was to provide critical medical history information to health providers in times of emergency. These devices had significant limitations, including insufficient security safeguards and lack of interoperability, rendering them useless if the medical data could not be accessed. In addition these devices requires a special computer or software to read the data from them. Currently, the availability of smartphones has led a dramatic change in the landscape of mobile health solutions. The smartphone application market has extremely expanded almost in all fields including healthcare.

These applications are developed mostly based on leading platforms such as Android and iOS (Kharrazi et al., 2012). A comprehensive study has been performed throughout this research on PHR. Previous studies have been reviewed and analyzed in order to understand the current trends in PHR and its adoption level worldwide. The review conducted is summarized in Table 2.1.

Table 2.1: A Review on Personal Health Records (PHRs)

Author	Category	Description	Conclusion
(Tang et al., 2006)	Review and analysis	This paper summarizes the college symposium discussions on PHR systems and provides definitions, system characteristics, technical architectures, benefits, barriers to adoption, and strategies for increasing adoption.	PHR systems can be used to transform patient information specially when integrated with EHR systems. However, this study identified many technical, social, organizational, legal, and financial challenges that warrant further study. In overall, more PHR related research is required.
(M. Lee, Delaney, & Moorhead, 2007)	Design and development	This article focusses on designing and developing an Internet-based PHR, IowaPHR, in order to show how nursing can be integrated into the PHR.	Nurses can expand their roles in the hospital with the use of PHR. Through moving the field of nursing even closer to satisfy the needs of health consumers.
(Maloney & Wright, 2010)	Review and analysis	This article reviews the features of commercially available USB-based Personal Health Records (PHR) devices.	Study shows PHRs are important in the health care field. However, USB based PHRs appears to have deficiencies. Tethered or web-based PHRs may be a better option for patients.
(Cushman et al., 2010)	Comparative analysis	This article summarizes the issues raised by the first phase of HealthDesign projects. The issues have been categorized into four topics: privacy and confidentiality, data security, decision support, and HIPAA and related legal-regulatory requirements. These issues will be helpful to achieve successful PHR.	Project HealthDesign cleared that: (a) Significant risks to privacy and confidentiality can be posed with the novel ways health information is shared and distributed using PHR. (b) In order to safeguard the health information, patients themselves play an unprecedented role in protecting their own heath records; and (c) Social and economic fears of patients must take into account while future PHR design and development.
(Archer, Fevrier-Thomas, Lokker,	Scoping review	This paper has reviewed the literature on PHRs. Design, functionality, implementations, applications, outcomes and perceived and real benefits of	This study showed the importance and benefit patients are getting when adopting PHRs. Some examples included easy access

Author	Category	Description	Conclusion
McKibbon, & Straus, 2011)		PHRs have been described according to an emphasis on experience in the USA and Canada. It was found that because primary care physicians play a key role in patient health. PHRs are likely to be linked to physician electronic medical record systems, hence; PHR adoption is dependent on growth in electronic medical records.	to test results, better communication with healthcare practitioners and reducing the need for inter-provider communications to access updated medical information. In overall conclusion more research is required that aware users the optimum functionality and usability of PHR systems, and how they can play a valuable role in underpinning self-managed healthcare.
(Kharrazi et al., 2012)	Evaluation & Assessment	This article evaluates some mobile PHR applications (mPHR) for the three leading cellular phone platforms (iOS, BlackBerry, and Android) Nineteen mPHR applications (8 for iOS, 5 for BlackBerry, and 6 for Android) were identified and evaluated. Assessing each for content, function, security, and marketing characteristics.	Astonishingly seven mPHRs missed the basic and most important security measures such as password protection; in addition none of the mPHRs apps contained all attributes included in the evaluation. The cost of the apps was not expensive. In overall conclusion the author expected in the near future, due to expanding the mobile market, more comprehensive mPHRs apps will be developed.
(Ming, Shucheng, Yao, Kui, & Wenjing, 2013)	Framework	In this paper a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers have been proposed. The main framework was designed based on outsourcing the PHR on third party cloud service providers.	To ensure complete control of their own privacy, patients shall encrypt their PHR files. Challenges have been addressed such that the complexity of key management has been greatly reduced in this framework while enhancing the privacy is guaranteed compared with previous works.
(Genitsaridi, Kondylakis, Koumakis, Marias, & Tsiknakis, 2013	Review and analysis	This paper presents an evaluation study on PHR systems that provides an overview on their current status with regard to functional and technical capabilities.	The author has recommended several points in order for patients to afford adopting PHR systems. Such as it should be free and open source, secondly the PHR system should be web based in nature in order to simplify the process of integration with mobile and tablets. At last the PHR system should be highly fully functional and secure product.
(Tansel, 2013)	Review and analysis	This article reviews NHIN the heterogeneous distributed system infrastructure for medical service delivery in the U.S.	Patients' health records are digitally available and can be electronically exchanged among related parties, doctor notes and prescriptions can also be electronically recorded. However, these data remains neither complete, nor up-to-date. However, when these

Author	Category	Description	Conclusion
			data are given to the patient "PHR" it will become complete and related information for a patient. Hence, PHR provides a base that fosters innovation to improve quality of health care and reduce costs.
(Ant Ozok, Wu, Garrido, Pronovost, & Gurses, 2014)	Evaluation & assessment	This article studies the usefulness and usability of web based PHR systems. The study has been conducted in a multi-method descriptive way including direct observations, concurrent think-aloud, surveys, interviews and focus groups in selected clinic.	It was observed throughout this study that the majority of the patients found PHR system useful and easy to understand except for elder patients who found it quite difficult to understand. Health providers as well found this web application very useful due to its positive impact on patient activation. The author at last suggested future PHR systems should be better in integration with hospital systems; security aspects should be concern and should offer more tailored health information.
(Tom et al., 2014)	Evaluation & assessment	This study determines the association of parental use of integrated personal health records (PHRs) with children's adherence to immunization.	The author has observed that PHRs can help in ensuring that the children receive timely preventive care, such as immunizations. PHRs can also help parents in scheduling the next appointments through the appointment management tools.
(Van Gorp, Comuzzi, Jahnen, Kaymak, & Middleton, 2014)	Framework	This paper proposed the use of MyPHRMachines the previously developed cloud based web service for healthcare. According to the author the proposed PHR platform satisfies not only the conventional requirements i.e. interoperability, security, and privacy but it also supports the opening innovation i.e. it presents the least possible impediments to the transfer of data and provides some control over the platform.	The MyPHRMachines platform allows different machines such as tablets mobile phones and computers to access to it and use it. According to the author patients can access to all their PHR data throughout their devices and they can view it. However, whether this approach can help in health information exchange on a nationwide level will remain a question mark.
(J. Liu, Huang, & Liu, 2014)	Framework	This paper has proposed an overview and analysis on several access control mechanisms. It was noticed that in best scenarios, data were stored on a commercial PHR system or outsourced to a third party data centre. Most of the existing access control mechanisms and sign-then-encrypt techniques are not suitable to be used in these	It was claimed by the authors that the new primitive Ciphertext-Policy Attribute Based Signcryption (CP-ABSC) satisfies the requirements of cloud computing scenarios for PHR. The proposed CP-ABSC can effectively realize fine-grained data access control in cloud computing. Furthermore, it provides a better trade-off

Author	Category	Description	Conclusion
		scenarios. Hence, a novel framework for secure sharing of PHR in cloud computing has been proposed in this paper.	between security and efficiency. Only authorized users are allowed to sign the PHR or designcrypt the signcrypted PHR. The future research lies in to design more efficient attribute-based signcryption schemes for mobile devices.
(Househ, Borycki, Rohrer, & Kushniruk, 2014)	Framework	The main objective of this paper is to introduce a framework to help people in understanding the proper use "meaningful use" of PHRs and to discuss the associated challenges that faces the proper use of PHR such as health care regulatory and managerial policies and multiple institutional, societal, cultural, and economic issues. Additional challenges, such as technology, design, usability, and implementation, still exist that relate to socio-technical issues.	According to author meaningful use of PHRs by health consumers and patients is a new research area which remains explored. Yet many PHR programs have not investigated the issues and challenges of meaningful use, especially from a health consumer perspective. This paper provides a conceptual framework for understanding meaningful use and provides details on the associated health care system and socio-technical challenges important in reaching a state in which PHRs are meaningfully used by the health consumer.
(Genitsaridi, Kondylakis, Koumakis, Marias, & Tsiknakis, 2015)	Systematic review & evaluation	In this article a systematic review on currently available PHR systems is presented. The set of requirements for achieving efficient PHR system have been identified based on real world implementation of some European research projects and some highly used standards.	This study concluded that despite the growing number of PHR systems, there is still much more to be done in the existing PHR systems in order to achieve fully intelligent patient health self-management and sustainability. It was observed in the studied systems, most of them were unable to support important functions, such as appointment scheduling and appointment reminder and technological characteristics as well as their poor architectural designs which has caused obstacles to their maintenance, expandability and use.
(Y.-T. Song, Pak, Kalabins, & Fouché, 2017)	Framework	This paper proposes a personal healthcare system and a Raspberry Pi based clinical data measurement module. Patients can take full control over their own health data and also facilitate communications among all participants. The storage can be accessible from patients and physicians so both parties can contribute to the clinical information, which allows monitoring and control of personal health.	The system utilizes personal cloud storage where each patient stores his/her data in a standardized format such as SNOMED CT, ICD10, HL7 CDA, etc. and such storage is completely independent from any applications so patients can own their own clinical information regardless of types of medical insurance plan, hospitals, or doctor's office.

From the 16 articles listed in Table 2.1, it can be concluded that more PHR related research is still required in order to address the various limitations encountered so far in PHR systems. Several suggestions have been proposed in order to improve PHR services including web-based PHRs, cloud computing PHRs, Mobile and tablets based PHR (mPHR) and finally a distributed approach towards sharing PHRs was recommended. Some articles discussed the benefits patients are getting when adopting PHRs provided that patients are aware of the functionality and usability of PHR systems. However, some mPHR systems missed the basic security measures such as password protection. It was also recommended to apply encryption standards in order to ensure complete control of patient's privacy.

2.5 Enabling Technologies

In order to achieve the efficiency in data transmission with satisfaction of the security requirements, the technology that will be implemented must be simple to adopt, fast, human centric and convenient with greater immunity against any possible attack such as man in the middle attack, sniffing and eavesdropping (Passwords, 2011). In the next section the data connectivity and transmission technologies that satisfies the requirements is discussed in depth and the security technologies is revised and discussed.

2.5.1 Connectivity Options

The advancement in the communication and connectivity technology in earlier days opened the way for important telemedicine applications and new e-health services, i.e. the use of wireless communications technology for medical service delivery. Recent advances in wireless communications networks led the way to direct and flexible healthcare to patient cases that could not be efficiently served with the traditional wired

communication systems (Batistatos, Tsoulos, & Athanasiadou, 2012). Nowadays, the development in the mobile wireless connectivity technologies such as Near Field Communication (NFC), Bluetooth and Wireless Fidelity Peer to Peer (Wi-Fi P2P) can participate in delivering medical assistance and can also support in emergency situations at the time when patient arrives at the hospital. In the next section, a detailed description is given to various connectivity options available in most of the modern smartphones.

2.5.1.1 Bluetooth & Wi-Fi

IEEE 802.15.1 – Bluetooth and IEEE 802.11 Wi-Fi are for short-range wireless communication protocol standards which consumes low power. Each of this protocol intended for different applications. For example, Bluetooth is widely used in cordless mouse, keyboard, and hands-free headset, while Wi-Fi is directed at computer-to-computer connections an alternative for cabled networks (J. S. Lee, Su, & Shen, 2007).

(a) ***Bluetooth***

Bluetooth is a technology designed based on wireless radio system mainly to connect computer peripherals such as mouse, keyboards, joysticks, and printers replacing the traditional cables. This range of applications is known as wireless personal area network (WPAN). Bluetooth works mainly on two connectivity topologies: the piconet and scatternet. A piconet is a WPAN formed by a Bluetooth device serving as a master in the piconet and one or more Bluetooth devices serving as slaves. Devices are synchronized using the clock of the master while communicating with each other in a given piconet. Slaves communicate only with their master in a point-to-point fashion under the control of the master. The master's transmissions may be either point-to-point or point-to-multipoint. Slave device can be either in active mode or standby mode in order to reduce power consumptions. On the other hand two piconets can be connected to form a scatternet. One Bluetooth device may participate in several piconets at the

same time, thus allowing for the possibility that information could flow beyond the coverage area of the single piconet (J. S. Lee et al., 2007).

(b) ***Wi-Fi***

Wireless fidelity (Wi-Fi) is a wireless communication technology that has a number of uses. However, it's most widely used for internet access (WLAN). Almost all smartphones, mobile devices and laptops has Wi-Fi enabled in them allowing the users to surf the Internet at broadband speeds when connected to an access point (AP).

There are several components in the architecture of IEEE 802.11 that are involved in interacting with each other to provide a wireless LAN in order to supports station mobility transparently to upper layers. IEEE 802.11 LAN defines a Basic Service Set (BSS). When the station moves out of its BSS, it won't be able to directly connect or communicate with other members of the BSS. Based on the BSS, IEEE 802.11 employs the independent basic service set (IBSS) and extended service set (ESS) network configurations. Beside internet usage, Wi-Fi technology can also be used to connect two devices and enable them to share data or even network resources, in this case, it is called Wi-Fi Direct or Wi-Fi P2P. Compare to Bluetooth technology, Wi-Fi Direct is faster and much easier to configure.

2.5.1.2 Near Field Communication (NFC)

Near Field Communications (NFC) is a short-range wireless technology that was developed by Philips and Sony for contactless communication. Allowing NFC enabled devices to actively interact with each other. This technology is built upon Radio-Frequency Identification (RFID) and is standardised in ISO/IEC 18092. It enables the stored data to be read instantly at a short distance up to 10 cm between the two devices. NFC is intended to make it easier and more convenient to make transactions, exchange digital content, and connect electronic devices with a touch. NFC devices have a higher

degree of security because both sniffing communications and man-in-the-middle attacks are then harder if not impossible to accomplish. NFC involves an initiator and a target. The initiator initiates and actively generates an RF signal and controls the exchange of data where the request is answered by a passive target (Curran, Millar, & Mc Garvey, 2012).

NFC technology uses the following smart devices:

a) **NFC-Enabled Mobile Phone:** Nowadays NFC technology is available in most of smartphone devices. The most common use case scenarios, users' mobile devices will scan, acquire and act upon the available data, connect and exchange data with other devices. In recent years, NFC technology is being increasingly considered as a solution for contactless mobile payment services (Luo, Yang, & Huang, 2016).
b) **NFC Reader:** This has the capability to transfer data with another NFC component. Most common example is contactless point of sale (POS) terminal. Which performs contactless payments when an NFC device is touched against the NFC reader.
c) **NFC Tag:** NFC tag is actually an RFID tag that has no integrated power source.

NFC devices immediately start their communication when they are touched. The touch action is actually taken as triggering condition for NFC devices to start communicating. In this review, android operating system based smartphone devices are selected. Android allows sharing or exchanging data using NFC technology between either two android powered devices or an NFC tag and an android powered device. Android with NFC enabled devices supports three modes of operation.

1. **Read/Write mode:** This allows NFC device to read/write passive NFC tags and stickers. This mode is usually about communicating NFC-enabled mobile phone with NFC tag for the purpose of either reading or writing data to those tags. Hence, there are internally two modes defined, reader mode and writer mode. In reader mode the initiator reads data from a 13.56 MHz NFC tag. The NFC tag will be consisting the requested data as well as the program that returns the requested data to the initiator. On the other hand, in writer mode the mobile phone initiates and writes the data to the tag. If the tag already contains some data, depending on the algorithm, these data will be either overwritten, updated or modified. The mobile phone after reading the data from the tag, it can perform different actions, for example if the tag stores URL the mobile phone launches automatically the web browser and displays the received web page. The features available in mobile phones such as processing power, audio/video capability, and internet access provides many opportunities for users and service providers when read/write mode is used. Hence, applications in this mode are countless and can be very innovative.
2. **P2P mode:** This mode allows an NFC enabled device to exchange data such as contact record, text messages, pictures or any other type of data with another NFC enabled peers. This mode has two standardised options: NFC Interface and Protocol (NFCIP-1) and Logical Link Control Protocol (LLCP). In most of the cases this operation is completed by Android beam.
3. **Card emulation mode:** This mode allows the NFC device itself to act as an NFC card. The emulated NFC card can then be accessed by an external NFC reader such as an NFC point-of- sale terminal.

Advanced NFC concepts enables the use of various technologies that android supports, especially when NDEF (NFC Data Exchange Format) are not used. In this

case one should define its own protocol stack. Hence, android provides support to detect certain tag technologies and allows communication with the tag using the defined protocol stack.

2.5.1.3 Comparative Summary

Table 2.2 summarizes the overall features of the above discussed connectivity technologies which are commonly available in most modern smartphones, tablets and other handheld devices. USB has been also taken into consideration as a connectivity option since it has the capability to connect smartphone or tablet to any other electronic devices such as laptops and digital cameras.

Table 2.2: Comparison of connectivity options

Technology	USB	Wi-Fi P2P	Bluetooth	NFC
Speed/Data Transfer Rate	1.5 Mbits/s – 480 Mbits/s	54 up to 200 Mbits/s	Up to 721 Kbit/s	Up to 424 Kbit/s
Coverage/Range	Wired connection 3-5m	50-100m	10m (up to 100m)	Up to 10 cm
Frequency	--	2.4 – 5GHz	2.4 – 2.5 GHz	13.56 MHz
Power Consumption	100 – 500mA	Related with range	<15mA	<15mA
Primary Devices	Computer peripherals, network adaptors, portable media players, etc.	Smart phones, tablets, Notebook, etc.	Smart phones, tablets, Notebook, etc.	Smart phones, tablets, Notebook, etc.
Usability	Requires device compatibility with OS.	Setup is required prior to use	Not convenient due to long setup time	Intuitive, Human centric easy, convenient, fast
Network Configuration	Host direct	Peer to peer	Point to Multipoint	Peer to Peer
Communication Mode	Half duplex	Active – Active	Active - Active	Active – Active Active - Passive
Set up Time	Variant by device	Variant by device	~6 S	< 0.1 S
Applications	Transferring data, connecting devices.	Sharing data, synchronizing data, playing games, videos, androids.	Data exchange, head set.	Connectivity, data exchange, RFID, payment

Technology	USB	Wi-Fi P2P	Bluetooth	NFC
Security	Low	Good	Good	High
Security Level	--	Supports using WPA2 (AES - CCMP)	Protocol Level	Hardware and protocol level
Network Standard	--	IEEE 802.11	IEEE 802.15.1	ISO 13157

Each connectivity option has its own merits and demerits. The Wi-Fi P2P and USB options have high speed data transfer rate. However, Wi-Fi has wide coverage range, therefore subject to security breach and USB option as well has drawbacks such as device compatibility with OS and even sometimes driver installation might be required to allow the device to get connected with the system. Comparing all the available options, it's concluded that NFC has better security feature since the coverage range is within 10 centimetres makes it difficult for any attacker to sniff while the transmission is happening. On the other hand, NFC nowadays is a new trend in transmission technology that most of the smartphone manufacturers insists to enable it on their devices.

2.5.2 Security Options

The capability of smartphones in hosting various types of multipurpose applications ranging from banking, email, text editors, health, business and social media applications, made them an attractive target for various type of security attacks. In addition, the advanced programming capabilities provided by the smartphone platforms to the application developers have compromised the security and privacy of the device holder (Mylonas, Dritsas, Tsoumas, & Gritzalis, 2011). In the following subsections, a brief discussion on some of the security mechanisms including lightweight encryption and hashing algorithms that can be applied on smartphone devices are discussed in detail.

2.5.2.1 Encryption Algorithms

In cryptography, the term encryption refers to conversion of an electronic data from a form that is readable to an unreadable format called ciphertext, which cannot be easily understood by anyone except authorized parties. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via any means of data transmission technologies. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications. Encryption is the key component of securing any data. Some of the popular existing encryption algorithms are discussed in this section. In order to adopt a proper security algorithm in any healthcare framework, a review in the following section is briefly conducted on available encryption algorithms that are supported by some smartphone platforms. These algorithms were evaluated against the common security properties which are confidentiality, integrity and availability abbreviated as (CIA).

(a) ***RSA Algorithm***

RSA is one of the most widely accepted and implemented public-key, block-cipher encryption algorithms, developed in 1977 and first published in 1978 (R. L. Rivest, Shamir, & Adleman, 1978) by Rivest, Shamir and Adleman (hence the acronym). It is based on the idea that factorizing integers into their prime factors is hard. In practice, RSA has proven to be effective, as long as it is implemented correctly. Despite the fact that several attacks have been reported over the years, they mostly illustrate the dangers of improper use of RSA (Boneh, 1999). However, the proper implementation of security algorithms is always a nontrivial task. Besides the general brute force attack, known attacks on RSA include mathematical attacks (Salah, Darwish, & Oqeili, 2006), side-channel timing attacks (Kocher, 1996), and short plaintext attacks (Boneh, Joux, & Nguyen, 2000). Boneh (1999) discussed other various type of attacks on RSA. To defend against integer factoring and brute-force attacks, large key sizes should be used.

Because the complex computations involved in encryption/decryption and key generation, slower performance is expected from larger key spaces. Public-key cryptography in general is inferior to private-key, symmetric cryptography, and RSA is around thousand times slower than the older DES algorithm (Diffie, 1988). Public-key cryptography, such as RSA, usually requires additional computational power and should be used with caution to avoid draining the battery of the device (Y. Wang, Streff, & Raman, 2012). RSA is used mainly for key management and digital signatures applications.

(b) ***ECC***

Elliptic curve cryptography (ECC) is an approach to public-key cryptography, based on elliptic curves over finite fields (Koblitz, 1987). ECC is a more recent competitor to RSA, first proposed individually by Neal Koblitz and Victor Miller in 1985. The main advantage of ECC over RSA is that it offers equivalent security with smaller key sizes, which results in faster computations, lower power consumption, as well as memory and bandwidth savings (Gupta, Gupta, Chang, & Stebila, 2002). This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. With a 160-bit modulus, an elliptic curve system offers the same level of cryptographic security as RSA with 1024-bit. The smaller key sizes result in smaller system parameters, smaller public-key certificates, bandwidth savings, faster implementations, lower power requirements, and smaller hardware processors (Jurišic & Menezes, 1997). Apparently, the only advantage of RSA over ECC is that the latter cryptographic applications have been noticed recently and the former is much more ubiquitous and tested. RSA has been well-researched and has been the topic of many seminal theses (Kapoor, Abraham, & Singh, 2008).

*(c) **NTRU***

NTRU was introduced in 2009 as a new standard for public key cryptography. NTRU features reasonably short, easily created keys, high speed, and low memory requirements. NTRU encryption and decryption use a mixing system suggested by polynomial algebra combined with a clustering principle based on elementary probability theory (Hoffstein, Pipher, & Silverman, 1998). NTRU has several advantages compared to RSA and ECC such as similar security level with smaller key size, faster speed, faster key generation and less computation power. NTRU is fast compared to RSA and ECC; however, as expected from a public-key cryptography algorithm, it is around 20 times slower than AES (Hermans, Vercauteren, & Preneel, 2010). While factoring and discrete logarithm based cryptography continue to dominate the market, NTRU family of cryptographic algorithms are the most practical alternatives that are not vulnerable to attacks using Shor's Algorithm (Perlner & Cooper, 2009), and hence appears to be resistant to quantum attacks. In a nutshell, public key algorithms are mainly used when there is a requirement for encryption, authentication, and non-repudiation along with verification of data integrity. In a comparison, the fastest asymmetric algorithms is at least 20 times slower than symmetric algorithm.

*(d) **AES Algorithm***

The Advanced Encryption Standard is an encryption specification established by the U.S. National Institute of Standards and Technology (NIST). In 2000, NIST selected Rijndael algorithm (Daemen & Rijmen, 2013), developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen for this standard specification (Standard, 2001), after a three-year competition. Rijndael algorithm is a symmetric block cipher that can use cipher keys with lengths of 128, 192, and 256 bits. AES is the best known and most widely used block cipher. While for AES-128, there are no known attacks faster than exhaustive search, AES-192 and AES-256 were recently

shown to be breakable by attacks which require 2^{176} and $2^{99.5}$ time, respectively. However, these attacks are completely non-practical or applicable only with respect to reduced versions of the standard, therefore do not seem to pose any real threat to the security of AES-based systems (Biryukov, Dunkelman, Keller, Khovratovich, & Shamir, 2010). AES is a fast cipher that works very well across all platforms (Schneier et al., 1999). A disadvantage of this algorithm is that, being a symmetric algorithm, it requires secure channel to exchange the encryption keys.

(e) ***Blowfish (Cipher)***

Blowfish is a symmetric block cipher developed by Bruce Schneier in 1993 (Schneier, 1994a, 1994b). It is a fast, compact and simple cipher. It takes a variable-length key, from 32 bits to 448 bits. It is only suitable for applications where the key does not change often, like a communications link. Since its introduction in 1993, the Blowfish algorithm has come to be regarded as a strong algorithm. However, some attacks are possible for certain poor choices of keys (Gonzalez, 2007).

(f) ***RC6***

RC6 is another type of symmetric key block cipher which was designed to meet the requirements of AES (Ronald L Rivest, Robshaw, Sidney, & Yin, 1998). RC6 was based on RC5 (R. Rivest, 1995), with modifications made to meet the AES requirements, increasing the security, and improving the performance. RC6 was designed to thwart theoretical attacks published on RC5. The algorithm was one of the five finalists in the AES competition and is patented by RSA Security.

2.5.2.2 Hashing Algorithms

Hashing algorithms are well known in computer science. A hash algorithm is a function that converts a data string of an arbitrary size to a string of a fixed size known as hash value or message digest. Any change to the message should change the hash

value. Therefore, hashing is widely used in ensuring the integrity of data. A hash function is designed to be a one-way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Hashing is also being used in data hiding techniques. Nowadays, passwords are not stored anymore in plain text. Instead, they are hashed and the hash values are stored inside the database. This practice protects the passwords from being exposed in case if the database is compromised. In the following section few popular hashing algorithms that are supported by some smartphones platforms are discussed in more detail.

(a) ***MD5***

MD5 is an acronym for Message Digest, it is an improvement of MD4 which was designed in 1992. It was one of the most widely used cryptographic hash function. There were several powerful attacks against MD5 which allowed to find collisions efficiently (X. Wang & Yu, 2005). Therefore, it's not suitable for applications like SSL certificates or digital signatures that rely on this property for digital security. Further advances were made in breaking MD5 between the year 2005 and 2007 making further use of the algorithm for security purposes questionable.

(b) ***SHA-1***

SHA-1 is an acronym for Secure Hash Algorithm and it was designed by the US National Security Agency and published as a secure standard by NIST in 1993, then revised in 1995 (Burrows, 1995). This Standard specifies a secure hash algorithm for computing a condensed representation of a message or a data file. When a message of any length < 264 bits is input, the algorithm produces a 160-bit output called a message digest. SHA-1 is the most widely used among the existing three SHA hash functions.

SHA-0, SHA-1, and SHA-2. Since its publication, SHA-1 has been adopted by many government and industry security standards for digital signatures and as an important component in other cryptographic schemes and protocols, such as user authentication, key agreement, and pseudorandom number generation. Collision search attacks on SHA-1 was shown to be possible 2000 times faster than brute force (X. Wang, Yin, & Yu, 2005), which suggests that the algorithm is not secure enough for ongoing use in the future, and hence the move towards SHA-2 and more recently SHA-3 is encouraged.

2.6 Current Solutions in HIE

Despite the conceivably enormous benefits of EHRs, one major drawback remains an unresolved issue. The heterogeneous mixture of involved health providers, each with its own adopted technologies and policies leads to a lack of interoperability. It is very difficult to share patient and healthcare information across providers' boundaries, and it is very likely that even when such sharing could be achieved, incompatibility between system formats and coding would render this exchange useless.

What the current situation does resemble is more of a fragmentation problem, where data is fragmented over many sectors, and as a result the global context of the health information is missed out and lost great potential advantages. This fragmentation is a fundamental contributor to increased spending and poor overall performance of the healthcare system (Benli et al., 2012). The result is lack of accountability, medical errors, waste and duplication. On the other hand, the ability to interchange health information among interoperable electronic records systems leads to an improved healthcare quality and efficiency, in addition to many other rewards for research and health management.

Potential stakeholders to take advantage of this data exchange include hospitals, skilled nursing facilities, clinics, private physicians' offices, pharmacies, laboratories,

radiology facilities, health departments, and the patients themselves (Shapiro et al., 2006). Health information exchange could make emergency care less expensive, more efficient, and safer for patients (Shapiro et al., 2006). If put in a nationwide context, the benefits are conceivably rewarding to the point that, as phrased by (Walker et al., 2005), "there is a business case to be made for spending money on a fully standardized nationwide system".

Researchers even suggested the comparative case of health information networks to the shipping and banking business (Shapiro et al., 2006). In the condition of significant investments by both private and public sectors, authors in (W. Liu et al., 2012) expected those solutions to experience the same advances in other industries like telecom, when they were deployed in the past. The most relevant works on general aspects in HIE including security, exchange, challenges, and benefits have been reviewed and summarized in Table 2.3.

Table 2.3: A review on Health Information Exchange (HIE)

Author	Category	Description	Comments
(Burton, Anderson, & Kues, 2004)	Review & analysis	This article summarizes the different organizations in the United States that are using securely EHR technology to transmit medical data. Barriers: - 1. No common format or standard for recording clinical information 2. High cost implementation and maintenance 3. Patient's privacy loss while information sharing.	The author has offered three recommendations for HIE, 1. Physicians and leaders should agree on common health record. 2. Regional governance structures that encourage HIE should be established. 3. Insurers and managed care plans should pay for using EHRs.
(Khoumbati, Themistocleous, & Irani, 2005)	Review & analysis	This paper has explained the importance of health integration and discussed the different integration technologies such as Enterprise Application Integration (EAI), Electronic Data Interchange (EDI) and Web Services. A comparative analysis of these technologies is presented along with its advantages and disadvantages.	The author has recommended EAI to provide the support for several HIE factors such as maturity, flexibility, scalability and portability. However, there is no practical or real implementation or experiment to prove the claim.
(Shapiro et al., 2006)	Review & analysis	This article describes the background and motivation for current regional health	It is obvious that for successful implementation of health information exchange, the

Author	Category	Description	Comments
		information organization efforts, and some specific issues that are likely to affect emergency physicians.	following issues must be addressed: (1) availability of electronic data, (2) data standards, (3) regional health information organization technical architecture, (4) financial, (5) privacy, and (6) public health and research.
(Sprivulis et al., 2007)	Review & analysis	This paper performs analysis and suggests savings of over two billion dollars annually from implementation of health information exchange in Australia.	The overall cost has been estimated based on peer-to-peer model of information exchange. To achieve the estimated benefits, all Australian health providers would need to participate in the network. However, Australian experts considered it unlikely that Australian health providers would be willing to undertake the substantial investment to upgrade their information systems to achieve interoperability in the absence of significant Australian government incentives.
(David C. Kaelber & Bates, 2007)	Evaluation & assessment	This paper provides an overview of six different ways in which HIE can improve patient safety. According to the authors, HIE participates in improving medication, laboratory, radiology and public health information processing and communication among providers and between patients and providers.	The authors has mentioned about one challenge that will face the development of HIE such as developing healthcare systems capable of processing and utilizing the dramatic increase in information. However, this is not the only problem, there are several problems such as security, interoperability, scalability and availability that will be faced by HIE in order to be fully implemented.
(Brian E Dixon, Zafar, & Overhage, 2010)	Evaluation & assessment	This paper describes a framework for evaluating the costs, effort, and value of nationwide data exchange as the NHIN moves toward a production state. The paper further presents the results of an initial assessment of the framework by those engaged in HIE activities.	This study has been done to encourage stakeholders such as hospitals and physician practices to develop an interoperable nationwide health information network (NHIN). This evaluation is important since it enables HIE organizations to demonstrate value to their stakeholders. However, whether all the stakeholders will be able to afford the cost of implementation will remain a question.
(Huang et al., 2010)	New proposals	Clinical Document Architecture (CDA) published by Health Level 7 (HL7) organization for exchanging documents among heterogeneous systems and improving medical quality. However, when exchanging	This does not allow the physician to retrieve the patient's record in real time through internet but it allows the records to be retrieved offline through a portal device such as USB. However, it has

Author	Category	Description	Comments
		medical messages many issues arises such as patient privacy, network security, budget, and the strategies of the hospital. This article proposes a method for the exchange and sharing of clinical documents in an offline model based on portable CDA.	been proved by previous studies that USB based PHRs currently on the market appear to have deficiencies. Therefore, Tethered or web based PHRs may be a better option for consumers at present.
(Som et al., 2010)	Review & analysis	Malaysia has started the initiative to implement E-health since July 1997. In 2004 Malaysian telehealth project was reviewed and the scope was reorganized into 7 components. In 2007 the structure of telehealth once again reorganized following the introduction of Integrated Health Enterprise (IHE) framework. The main problem raised was integration between one application with another. Considering the delay of implementation for this project, a new initiative was introduced in 2009 known as Malaysia Health Information Exchange (MyHIX).	The general view about Malaysian approach towards telehealth shows positive movements by the government and it also shows that the government is on the right track. However there is some delay in the execution and there are still more rooms to improve in the current application.
(Payne et al., 2011)	Review & analysis	This article describes the extensive initiatives in healthcare information technology that the UK has undertaken on a scale far larger than past or currently planned efforts in the USA. One of the goals of the most recent English health IT initiative is clinical information exchange on a national scale. Based on 37 individual interviews with patients only from England, the author concluded that UK has thus made enormous progress toward enabling clinical information exchange while also assuring policies of protecting data and regulated access control.	In UK printed prescription of the patient is generated and given to the patient, and the details of the prescription are transmitted to a central server on the spine. The UK approach towards HIE uses centralized server based approach. However, the US approach towards HIE faces several issues such as inconsistent participation across providers due to lack of interoperability between the health providers.
(Fontaine, Ross, Zink, & Schilling, 2010)	Review & analysis	More than 60 articles related to HIE were reviewed and tabulated. Issues related to HIE has been addressed in such a way that it could be adopted in the NWHIN to become a reality.	Several benefits of HIE were discussed based on the literature such as efficient workflow, improved quality care, cost savings and increased revenue. These studies were concerned on the patient in the United States. This review highlighted the importance of privacy and security of patient's health records without reviewing any previous solutions which can be adopted

Author	Category	Description	Comments
			in the current HIE.
(Vest & Gamm, 2010)	Viewpoint	The author discussed several issues regarding HIE in the United States. All the discussions were based on US experience with the HIE for the last two decades. The author has warned of repeating the mistakes of the past again. Due to the new technologies introduced people now cannot afford to wait longer to achieve HIE for their medical records.	The author mentioned about the importance of PHRs. However, PHRs still require technologically capable and willing exchange partners. According to the author's opinion, PHRs cannot completely ignore organizational behaviours. Individuals may benefit from increased access and control to their personal health information
(Frisse et al., 2011)	Evaluation & assessment	This paper examines the financial impact of health information exchange (HIE) in emergency departments (EDs). The results showed that HIE access reduced the overall costs including head CT use, body CT use, and laboratory test ordering.	This study demonstrated a positive financial impact on communities, however, the economic benefits will be only realized when the digital healthcare delivery system evolves.
(Lenert et al., 2012)	Viewpoint	This article explores the changes in policy toward health information exchange under the Obama administration especially when the US has invested $30 billion USD in the Nationwide Health Information Network (NwHIN) and electronic health records systems.	The author visualized several changes in the strategy for implementation of the NwHIN in the US including rise of private network for HIE.
(W. Liu et al., 2012)	Overview	This paper identifies the major challenges in eHealth interconnection network services. An overview of a solution framework is summarized with the aspects of interconnection services, operational management services, and security control services. This study has also documented the security challenges and QoS requirements while dealing with healthcare data.	The proposed solution has mentioned already known but useful points about the implementation requirements for insuring the security and privacy while transmission process of the health records
(Vest, 2012)	Review & analysis	This article provides a review of the current state of HIE in 7 nations, North America, Asia and Middle East, Australia and New Zealand, and finally Europe. The author founded fully functioning HIE is not yet a common phenomenon worldwide. However, multiple nations see the potential benefits of HIE efforts continue to work to overcome the challenges of interoperability, record linking, insufficient infrastructures, governance, and inter-organizational relationships.	It has been proved that international standards are not widely adopted in healthcare, instead health care organizations utilize self-developed standards for everything from diagnoses, to demographics, to charges. During the discussion section it has been mentioned about two aspects, emergency needs and patient-level specific planning, which suggests PHRs may be the most efficient means of international HIE in the majority of instances. PHRs do

Author	Category	Description	Comments
			pose the challenges of relying on patients to manage their information, but can be overcome if the PHR is linked to a clinical data source.
(Park et al., 2013)	Survey	A structured questionnaire survey has been conducted on patients in South Korea. 730 records have been collected. The survey was mainly focusing on HIE online through the exchange between the hospitals and offline such as a paper copy of the medical records	This study has shown positive impact on HIE by the customers. Although the survey targeted specific area of Seoul city with mostly technologically experienced patients however, the overall output results indicate that patient sentiment is ripe for implementation of HIE technology in South Korea to replace the traditional paper based medical reports
(Byrne et al., 2014)	Lessons and Findings	This study summarizes major accomplishments and contributions of Virtual Lifetime Electronic Records (VLER). The early lessons learnt from the health exchange as well as the implementation and evaluation, including findings related to adoption and perceived value of VLER Health Exchange to veteran patients and providers. VA commissioned a two year, independent evaluation and performance monitoring of the pilot phase to better understand the impact of VLER Health Exchange and to inform decisions about future directions for the program.	The pilot phase has started in December 2009 and completed in September 2012. 12 pilot sites were focused on this evaluation study. The feedback from the participants was positive. However the question is at the end of the day, is it possible for the 12 pilot sites to finalize and implement the real Veterans Affairs (VA) VLER system at their corresponding sites? If so, then is it possible to exchange data beyond the 12 pilot sites or even on nationwide basis. This article is lacking of more detailed technical details.
(Brian E. Dixon, Vreeman, & Grannis, 2014)	Overview	This article discusses three approaches for increasing semantic interoperability to support national goals for using health information technologies in the United States. First approach, data senders must use specific standards. In the second approach its receiver's responsibility to ensure the standardization. Finally in the third approach, the public health would collaboratively develop a strategic plan with data sharing partners.	It is mentioned by the author that the United States at present lacks a comprehensive strategy for full semantic interoperability of health IT systems. To achieve semantic interoperability, public health reporting and surveillance activities in the US, policies and standardized vocabularies must be adopted.
(Yeager, Walker, Cole, Mora, & Diana, 2014)	Evaluation & assessment	The purpose of this study is to examine the barriers and facilitators affecting the decision to participate in an HIE and, separately, which factors are affecting the use of HIE in Louisiana. This study was conducted in a single state (Louisiana) and, therefore,	Through previous studies, HIE participation have suggested that technical issues, costs, competitive concerns, data privacy and security concerns, and workflow implementation challenges, all prevents HIE participation. Conversely, studies have shown that

Author	Category	Description	Comments
		findings may not be generalizable across other state settings. It's also important to note that findings from this study were based on individual perceptions and opinions, which are limited to each individual's experiences.	technical assistance, financial incentives, hospital network membership, workflow integration and process redesign, and the inherent potential of HIE to improve quality of care delivery all facilitate HIE participation.
(Chen, Yang, & Shih, 2014)	New proposals	In this paper, a secure medical data exchange protocol based on cloud environment is proposed. Cloud characteristics were used to make it convenient for patients and doctors to use medical resources. Asymmetric encryption technology was used to ensure the privacy and protect the patient's information with mutual authentication which is based on pairing technology.	The proposed scheme can resist against the impersonation attack, replay attack, man-in-middle attack, stolen-verifier attack, and have known-key security. However, this article is mixing between three different areas such as HIE, PHR and cloud based security. Each of this area has its own security requirements. The proposed solution was mainly focusing on cloud based security while exchanging medical information.
(Eden et al., 2016)	Review & analysis	A systematic review of studies assessing facilitators and barriers the use of health information exchange (HIE) was done by searching MEDLINE, PsycINFO, CINAHL, and the Cochrane Library databases between January 1990 and February 2015 using terms related to HIE.	From this study, it was found that the most commonly cited barriers to HIE use were incomplete information, inefficient workflow, and reports that the exchanged information that did not meet the needs of users. Incomplete patient information was consistently mentioned in the studies conducted in the US but not mentioned in the few studies conducted outside of the US that take a collective approach toward healthcare. Patients and practices in the US have the right to either participate (or not) in HIE which effects the completeness of patient information available to be exchanged.
(Gibson, 2017)	Evaluation & assessment	This research has focused on the use of information systems to improve public-health or population-health outcomes. Organizational and technical aspects of HIE are discussed in detail along with a critical review on the value of HIE.	There is a huge gap between the potential of HIE and the current reality. After spending USD 31B on partially subsidizing EHRs, the US Congress is unhappy with the lack of data exchange among systems purchased by providers.

Table 2.3 lists articles that mainly focus on the issues related to HIE, spanning the period from 2004 to 2017. The list of papers indicates that many researches addressed

the importance of HIE and its wide-ranging benefits from patient's health point of view as well as its business aspects. Several articles also discussed and addressed different possible solutions to HIE problems. However, most of the proposed solutions are very general and discussed the issues in theory without concrete realizations that would validate the proposed solution. For example, there is still a large gap in the United States between the potential of HIE and the current reality, despite the huge amount of money spent by the government to enable data exchange among the different systems (Gibson, 2017) .

2.7 Chapter Summary

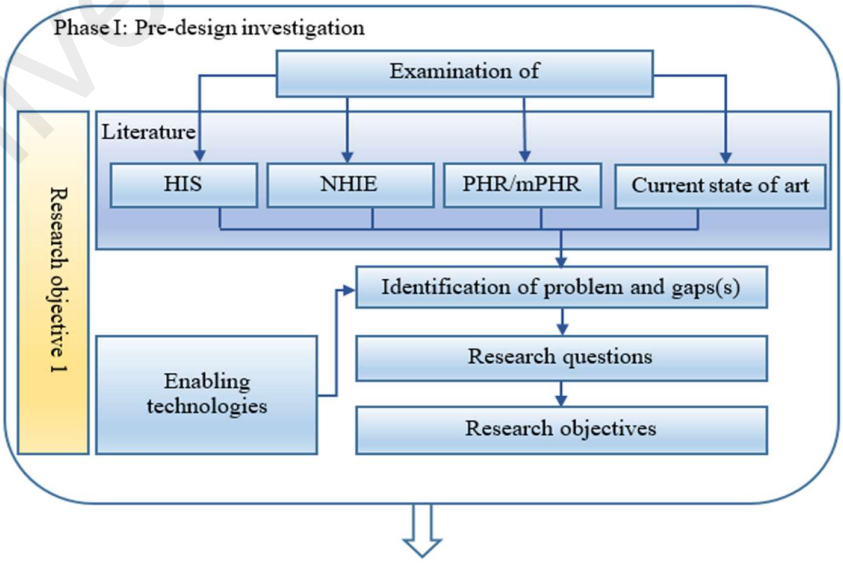
HIE is the key to the future of healthcare systems. Nations around the world have recognized this fact with strategic plans to achieve this goal. Malaysia is no exception. The Malaysian MOH has led and supervised the development of a consortium of pilot projects that cover all aspects of healthcare service delivery through the Malaysian Telehealth flagship project. Many barriers and obstacles emerge when HIE is applied on a national level. In particular, integration and interoperability are difficult challenges in the way of many nationwide experiments. Regardless of the approach used either "top-down" or "bottom-up", security and privacy requirements are crucial concerns when sharing or exchanging the health data of patients. The heritage of information security research is rich and capable of providing the desired solutions for secure integration, if the right mixture of technologies is employed. This chapter reviewed the basic concepts relevant to the literature of health information exchange, evaluated the most recent technologies that can enable data exchange and secure transmission, and finally summarized the state-of-the-art in HIE-related research.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter describes the methodological approach and research phases undertaken for conducting the present study. The adopted research methodology led to the division of the overall research work into four successive phases, each of which is described in a separate section.

3.1 Research Conceptual Framework

Conceptually, this research work comprises four distinct but interrelated phases. The first phase involves performing a general investigation of the current state of the art and the desirable needs of the suggested framework for health information exchange. The second phase provides the architectural design of the proposed framework and its interacting components. The third phase layouts the detailed implementation process of the prototypic proof-of-concept version of the proposed framework. Finally, the forth phase contains a series of validation tests for the implemented framework prototype. The overall conceptual framework of the research is depicted in Figure 3.1.



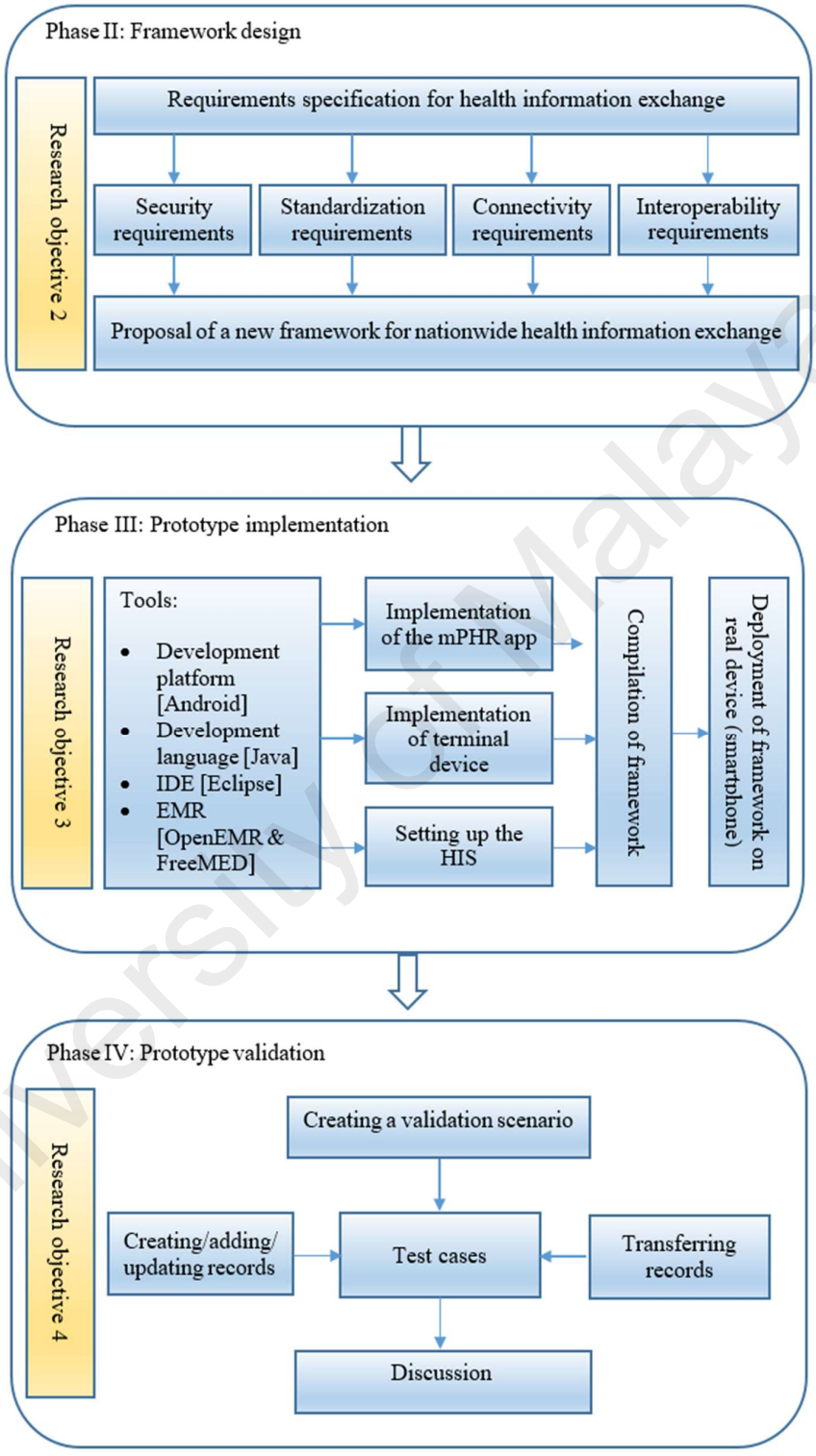


Figure 3.1: Conceptual Framework of the Research

3.2 Phase I: Pre-design Investigation

This phase laid the foundation for the rest of the work, identifying the research problem and the main concepts and technologies that are necessary to address the problem. To design a solution in the domain of health informatics, a number of distinct but related concepts and tools need to be investigated. Chapter 2 reviewed at some length four subjects that were carefully examined during the pre-design investigation phase of the research. The first subject is health information systems and their unique features that are common in any healthcare facility. The second subject is the exchange of health information and the potential benefits out of this process, as well as a few of the related issues. This thesis addresses the exchange of health information at a nationwide level, for which a number of current solutions exist though at a limited success.

The third target subject of the investigation phase is the technology of (mobile) personal health records. Finally, the pre-design investigation targeted the technologies that could be adopted in order to enable health information exchange on a nationwide level, using mobile PHRs. Finally the fifth domain includes the current state of art in context of health information exchange. The examination of all these aspects was instrumental to identify the specific problem that can be addressed by this research as well as the specific objectives that should be achieved to realize a working solution. As reflected from the first two chapters, the result of this phase directed the focus of this research work towards the design of an alternative approach for nationwide health information exchange to the available but less effective solutions.

3.3 Phase II: Framework Design

As stated earlier, the aim of this research is to develop a novel framework that provides an alternative solution for the problem of health information exchange. Based

on the finding of the preliminary investigation in the previous phase, several specifications have shaped out to constitute the desired framework based on the functional requirements such as interoperability and connectivity, non-functional requirements such as security and standardization demands, as well as the available enabling technologies.

Identifying the framework requirements led to the design of several components that are necessary to implement in order to achieve the desired needs. This multi-component design followed from the purpose of the framework, which serves several entities, including the patients and healthcare providers. To orchestrate all those needs, three main design components in the framework have emerged. The first component is an mPHR at the patient side, which is a smartphone app that carries the patient information and is also referred to as the "client"; the second component is the provider's Health Information System (HIS), which is typically a legacy EMR system that is expected to communicate with client mPHRs, and is also referred to as the "server"; and the third component is an interface device between the previous two components, which can be embodied using another mobile device with a special app to interconnect the clients with servers, and is referred to as the "terminal".

3.4 Phase III: Prototype Implementation

Based on the specified design in the previous phase, the purpose of this phase is to show whether, and how, the various components (i.e. clients, servers and terminals) as well as their operations might be realized. One of the important design goals of the proposed framework is that its deployment involves no changes to existing systems or infrastructure, and is possible using available hardware and software technologies. This goal is set to enable better acceptance of the proposed solution, and lower its barrier to adoption. In order to illustrate this fact, an initial prototypic proof-of-concept

implementation have been built for the various framework's components described in the previous phase.

One important and recurrent strategy has been followed throughout this phase, which is to adopt open source technologies whenever possible. For example, the open source Android platform was chosen to build the client and terminal apps, and open source libraries were utilized to implement various parts related to encryption and standards adoption. This decision contributes further to reducing the cost of implementing the proposed framework, among other benefits.

3.5 Phase IV: Prototype Validation

The implementation in the previous phase is only meant to serve as a proof-of-concept to validate the idea of the framework. To further illustrate the outcome of the resulting framework, a simple test scenario was performed in order to validate the different requirements that have been set forth during the design and implementation phases. The testing steps in this phase have covered the following main operations:

a. Registering a new patient at each terminal device.

b. Adding a new record to the provider's EMR system from the client mPHR.

c. Transferring the data back with updates from the provider's EMR system to the client mPHR.

d. Updating an existing record in the provider's EMR from the client mPHR.

3.6 Chapter Summary

This chapter outlines the general methodology that was adopted to carry out this research work. The research conceptual framework is presented in terms of four main phases. Each phase corresponds to a major distinct step in conducting the research,

towards producing the anticipated output. Beyond the phase of the preliminary investigation necessary to identify the research problem and main objectives, the chapter lists the major steps of designing the target distributed framework, implementing the proof-of-concept prototype of the framework, and then validating it based on simulated environment.

CHAPTER 4: FRAMEWORK DESIGN

This chapter introduces the structure of the proposed framework and describes its related components in detail. The first section of this chapter provides an overview of the main idea behind the proposed design. Next, Section 4.2 reveals the source of inspiration for the proposed solution to the problem of interoperability. Computer industry has long ago solved a similar problem of interoperability between peripheral devices and operating systems, and this section explains that analogy and shows how it can be applied to the problem of interoperability between various healthcare systems. The last three sections present the core of the design, including the overall architecture of the framework, the requirements and design of its component parts and the typical interaction between these components, respectively.

4.1 Overview of the Framework Design

The solution proposed in this thesis is essentially a framework that provides an alternative or complementary approach for government-centered projects. This framework is aimed to be practical, cost-efficient, and readily deployable, by innovatively using the available technologies, and requiring no changes to the current infrastructure or functional systems. The framework comprises several systems and related methods. The basic idea is that patient health information is carried by the patients themselves in the form of mPHR systems. These mPHRs run on their smartphones and may occasionally connect to the traditional electronic medical records (EMR) of healthcare providers.

Using mPHRs that move with the patients solves the problem of transmitting health information to places where they are needed. In this sense, the information itself becomes mobile and distributed. The original and up-to-date versions are stored where

they are needed the most, that is, with the patients. Redundant copies of the information are shared with healthcare providers when a patient visits them, and the most recent copy of the patient's information at a given provider is updated upon the next visit to that provider.

However, moving data around implies neither connectivity nor interoperability between incompatible systems. For this reason, the proposed solution suggests an operational model common to the computer industry, which is introduced in the next subsection. In essence, the actual connection between the mPHR of a patient and the EMR of a healthcare provider is done through a terminal device, which can be another smartphone or tablet. As long as the terminal device can speak the language of both systems, data exchange can occur with little or no change to any of them. Nonetheless, the terminal device has to support few more functions that are detailed in Section 4.5.2. Selection of a specific connectivity technology and supported data formats are implementation decisions that are discussed when describing the prototype implementation in Chapter 5.

4.2 Illustrative Analogy

The proposed distributed framework was inspired by the model of computer peripheral management. For a long time, only a few operating systems (OSs) dominated the personal computer market (e.g., Windows, Linux, and Mac OS). By contrast, the number of peripheral devices that connect to personal computers is much greater. New peripherals like printers, scanners, and webcams are continuously introduced to the market by different vendors. All these peripherals are generally expected to operate with an OS that is not aware of their internal design. Thus, there exists a problem of interoperability between the OS and every other peripheral device that is expected to

come out even long after the OS has been created, and yet plug into it and operate right away.

One possible solution is to ask vendors of OSs to update them with necessary functions to communicate with new peripherals. However, this is an impractical solution because of the number of new peripherals being produced and the difficulty of updating existing OSs. This is equivalent to asking a healthcare provider to change its legacy health information system (HIS) so that it is able to connect and interoperate with other HISs. The problem with this view is that each legacy system is seen as an operating system whilst other systems are the peripherals.

The solution implemented by the computer industry to the above problem is simple: the use of device drivers. Avoid the need to make new OSs omniscient or to modify existing operating systems by introducing an interface layer between the device and the OS. An interface is a piece of software used by the OS to communicate with a device. Manufacturers of the peripherals are now asked to provide this software (called a driver) along with their devices, to translate between their peripheral hardware and a particular OS. The rationale behind the model on computer peripheral management is that an OS cannot possibly know all the available peripherals in the market, much more cater to the intricacies and communication protocols for each of them. Hence, it is more appropriate for the peripheral manufacturer to provide the interface (driver) for its own device and ensure that it can correctly communicate with at least one OS using public Application Programming Interfaces (APIs).

In this research, a key point in the proposed framework is to view the HISs of various healthcare providers as the peripherals, not an OS. Subsequently, a single OS with well-known and public connectivity and data format should be established, so that each peripheral would know how to exchange information with that OS. In this setup, a

healthcare provider will just develop its own interface that can connect its legacy HIS to the new OS. The choice of this concept of global and unified OS, in the context of healthcare information, is to create a mobile PHR system that supports standard data formats and universal connectivity technologies. The interface between this mPHR and every legacy HIS is another device equipped with necessary software to play the role of device drivers. Each healthcare provider will only need to setup its device that can understand the unified format of the developed mPHR and the internal format of its HIS.

In this way, when a provider decides to start making use of the patient-owned mPHRs, it does not have to permanently join any network or connect to any particular server; neither does it have to share any part of its own database nor change any part of its legacy HIS to enable data exchange with patients. All it has to do is to develop basic software that can understand the (standard) format of incoming data from the patient's mPHR, and can translate that into the format used by the provider's internal HIS, and vice versa. Assuming that both this developed software and the mPHR are installed on modern smartphones, several connectivity options are already available for wireless data exchange.

Naturally, this process would be less attractive if done for a few patients only. The whole point here is to develop a single (or very few) mPHR apps(s) that are used by all patients, with a clear and well-known syntax of data format and semantics of exchanging the data. Once a healthcare provider sets up its interfacing device, it can virtually plug into a whole system of patient mPHRs.

4.3 Framework Architecture

The proposed framework encompasses several systems, methods, and internal interactions. The three main design components are as follows: an mPHR at the side of

the patient, legacy HIS at the side of healthcare providers, and an interface device between the two. The mPHR is referred to as the “client”, the provider HIS as the ‘‘server”, and the interface device as the ‘‘terminal”. The client is essentially a smartphone app that implements the function of a PHR system. The client forms the core of the framework; it primarily keeps the information of patients and carries it whenever needed. However, this core is not a central unit. Instead, it is distributed among all patients, where each patient maintains his/her own information via his/her client app. The clients can connect to the systems of healthcare providers through terminal devices, which are responsible for exchanging the information with the client on one side and the corresponding HIS of the provider on the other side.

In effect, the clients form a cloud of mPHR systems, with different healthcare providers plug into this cloud at certain points via terminals. Owing to the mobile character of clients, the cloud of clients can also be depicted as moving from one healthcare provider to next, as shown in Figure 4.1. The framework as a whole depicts a closed system in which individual components maintain only data of their own interest, and no single component holds the entire set of circulated information, as it is distributed over many storage/ processing units. If the government needs to obtain access to the complete set of information (e.g., for policymaking), it can hook into the framework, for example, through the HISs of healthcare providers.

It should be noted that fragmentation of health information is one of the problems that motivated HIE in the first place. In the proposed framework, however, this fragmentation is reorganized and deliberately maintained by design. Existing healthcare delivery practice suffers from fragmented pieces of a patient’s information that are hard to find or even know about at the right place and at the right time. By contrast, fragmentation in the proposed framework does not occur at the level of individual

patients. Full and up-to-date information of a patient is maintained in the mPHR client and exchanged when necessary with any HIS (server) via an interface device (terminal). The lack of a single repository for all healthcare information may also be attractive from management and security perspectives. Patients are more assured of their privacy if their information is kept only in their own smartphones and in the servers of their healthcare providers, not in a big and lucrative point of attack like a central database.

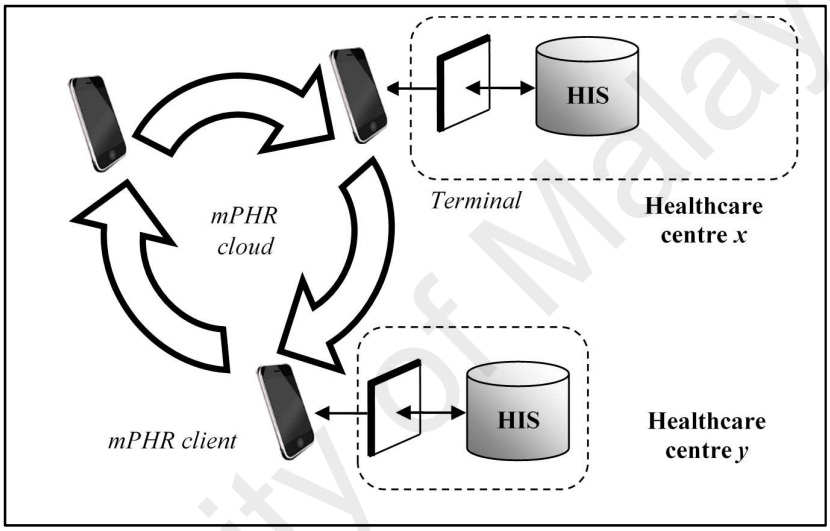


Figure 4.1: Proposed framework general architecture

4.4 Component Requirements and Design

Several requirements must be met for this framework to serve its purpose. In particular, the newly introduced client and terminal components should support the minimal functionality listed in the following subsections.

4.4.1 mPHR Client

The information of an individual patient is stored within a smartphone application (app for short). This app is a key storage and transmission unit of the framework. The client app interfaces with the patient and stores, maintains, and exchanges the information of a patient externally. The utilization of smartphones provides all the

necessary capabilities to fulfill the role of the client, namely, processing power, storage capacity, and connectivity. The client is taking the specific form and function of an mPHR that supports the following requirements.

(i) ***Friendly Graphical user Interface (GUI)***

The client app is to be used by the public and should provide an easy-to-use and appealing interface. A typical smartphone app allows the user to perform all functions via the touch screen using simple layouts, buttons, drop-down lists, menus, and similar user-interface elements. Advanced mPHR features can also be added, such as options to input data from external devices and medical sensors, and output options other than the screen, e.g., wireless printing.

(ii) ***Proper protection***

Medical data are among the most sensitive information that people save on their smartphones. The use of a proper encryption scheme to protect the information while at rest is important because smartphones can be lost or stolen. User authentication upon starting the app is also imperative to prevent tampering with the app in the absence of the real owner. Two points are important when managing encryption. First, using a standard encryption algorithm and not devising a custom method is essential. Second, a crucial part of any system that involves cryptology is key management. In the proposed design, the encryption and decryption of the stored health information occur on the patient device within the mPHR app. Thus, no keys have to be exchanged, and the same key can be used for both operations, leading to the use of a symmetric encryption scheme. Although the secret key need not be disclosed to any other party, it can still be revealed if stored along with the encrypted information and the device fell into the wrong hands. If the key is also encrypted, then a new key will be required for that

encryption and so forth. Combining authentication with encryption and adopting the scheme of password-based cryptography can overcome this problem (Kaliski, 2000).

(iii) ***Arbitrary but adequate format for saving medical data in a local database***

The format of the data within the mPHR client is unexposed to outside systems. Other systems see patient data only when exchanged in a standard format. Saving these data in a human-readable format is practical because these are personal health information meant to be managed primarily by the patient. Maintaining a diverse but related set of information entries, including their storage and retrieval, is a typical task of database management systems. Therefore, the proposed mPHR client app stores the health information in plain text using one of the database management systems that are supported on mobile platforms.

(iv) ***Method of translating between the internal representation of data and a standard format***

Referring to the previous analogy of peripheral devices and their drivers, the drivers must know how to talk to the OS for the whole model to work. This condition is achieved by writing the drivers for a specific operating system's API. The proposed framework follows a similar scheme. All healthcare providers setup a terminal device that expects to receive a specific format of information from mPHR clients. Instead of creating a new format to play this role, adopting an existing standard format for health information is appropriate. This approach ensures that everyone is (should be) familiar with the format and allows for the output information from the mPHR client to be used by other health information systems. Fortunately, such a standard for health data formats exists and covers every type of exchanged health information, including clinical and administrative data.

(v) ***Secure peer-to-peer communication technology to exchange information without relying on a preconfigured infrastructure-based network***

Several options for transmitting information from a mobile smartphone exist. In addition to the ability to connect via USB cables, all these options are wireless. The use of USB cables is obviously impractical and can render the exchange process unworkable in many cases. Considering the wireless options, some technologies rely on a basic infrastructure to enable communication between wireless devices and require the devices to connect to a single network managed by a central entity. Other wireless technologies enable devices to communicate on a one-to-one basis without any form of infrastructure. This form of communication is called peer-to-peer. A popular example of this category is Bluetooth and the recent technology of Wi-Fi Direct (Alliance, 2016).

The problem with these options is twofold. First, a configuration overhead associated with using these technologies always exists. In the case of Wi-Fi, the user must know the name of the correct network and, if the network is protected with encryption, must know the security key. In the case of peer-to-peer technologies, the communicating devices establish connection by engaging in a ‘‘pairing” process that requires the users of both devices to accept the connection and perhaps enter a PIN code.

The second problem with the aforementioned connectivity options is their ranges. Wi-Fi transmission can cover up to 100 m in every direction, whereas Bluetooth coverage can extend up to 10 m. These ranges are not required for peer-to-peer exchange of information but do allow for the interception of transmitted information by potential sniffers. The threat of eavesdropping can be mitigated by encrypting the communication, but this will introduce the problem of key management among the mPHR clients and the terminal devices, which is not a trivial problem.

From the above discussion, the desired attributes of the connection method for exchanging the information between the client and the terminal devices can be determined. Peer-to-peer communication is preferred to eliminate the requirement for any infrastructure with its necessary configurations. The transmission range must likewise be sufficient for the patient at the counter to pass information to the terminal device without exposing the information to a wider distance. The latter feature will allow for the exchange of plaintext information to be free from encryption overhead. A technology with these traits does exist, and is being introduced into modern smartphones at an increasing rate under the name of is Near-Field Communication (NFC).

As was explained in Chapter 2, NFC is a short-range wireless technology that typically requires an average distance of 4 cm or less to initiate a connection, with a maximum transfer speed of 424 kbps (Forum, 2016). NFC is based on the matured RFID technology but is integrated into modern smartphones. NFC is proved to be secure and stand against eavesdropping attacks especially if it is working in passive mode. In addition, there is no correct answer to question of how close an attacker needs to be in order to retrieve a usable RF signal. The reason behind that is due to huge number of parameters which determine the answer. For example, the distance depends on the following parameters and there are many more.

1. RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case and the environment).
2. Characteristic of the attacker's antenna (i.e. antenna geometry and the possibility to change the position in all 3 dimensions).
3. Quality of the attacker's receiver.
4. Quality of the attacker's RF signal decoder.

5. Setup of the location where the attack is performed (e.g. barriers like walls, metal or noise floor level).
6. Power sent out by the NFC device.

Therefore, any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines. NFC is considered one of the enabler technologies for future computing paradigms and is already found in a wide range of applications in academia and in industry, although not yet as popular as Wi-Fi or Bluetooth (Coskun, Ozdenizci, & Ok, 2015; Want, 2011). In the proposed design, NFC is selected for the main connectivity option between the mPHR client app and the terminal app, with the possibility of utilizing one of the other options when the amount of exchanged information is large (e.g., medical images).

(vi) ***Backup mechanism***

Adding the ability to import and export full or partial backups to the mPHR app is an important feature for at least two reasons. First, having a full copy of the mPHR database somewhere external to the smartphone is essential to avoid the data loss in the case of device theft or damage. The backup copy should be available for upload in a standard format [e.g., structured query language (SQL) script] to any online storage selected by the users, such as their cloud-based accounts, or offline storage on the device itself for later transfer. Then, users should also be able to download a previous backup copy to a newly installed mPHR app. Another advantage of being able to import and export all or part of the mPHR data is to prepare mPHR clients for any potential connection or integration with other HIE settings.

4.4.2 Terminal device

An important enabler of the proposed framework is the intermediate layer between the new mPHR client and the legacy HIS used by healthcare providers. The main purpose of this layer is to translate between the data format of the received information from the client app and the internal representation of the same information items inside the database of the HIS application. The translation can be done in software, which suggests that the function of this intermediate layer can be represented by another application (or a mobile app). Installing the new software on a separate device that can also communicate with client smartphones is appropriate, because the healthcare provider should supply this software with no impact on its existing system in any way. A device that has processing power and connectivity capabilities, in addition to being affordable and mobile, is just another smartphone (or tablet). A word ‘‘terminal” is used to describe the device, because it lies on the border between the client and the legacy system of the provider and provides access for both ends to each other.

Most often, the HIS database system is a relational database management system. The data in such databases are organized in a set of tables (relations), and the language used to read from and write to these tables is the popular SQL. According to the design of the proposed framework, all exchanged information between the client and the terminal are transferred in the form of standard HL7 messages, version 2 (HL7v2). The terminal device maps the fields in those standard messages into corresponding fields in the HIS database using the proper SQL statements. This mapping is also performed in the other direction when retrieving data from the HIS database to the mPHR client, upon patient discharge for example.

The requirements of the terminal are similar to those of the client component. The terminal requires a suitable user interface as a software app, although much less

sophisticated than that of the client. There is one exception to this simplistic interface requirement, however, which relates to authenticating patients. No patient should be allowed to send or receive health information that belongs to another patient, even when using the mPHR client of that patient. This requirement leads to the addition of a basic authentication functionality to the terminal along with a simple interface element to receive a password from the user. Considering that the terminal is not part of the HIS of the provider, the terminal should maintain the necessary information to authenticate the users of the different mPHR clients (i.e., the patients). The required information is minimal and can reside in a local database on the terminal device. This information includes the identity of the patient, a password, and some ways to map these data to the record of the patient in the internal HIS database, as depicted in Figure 4.2.

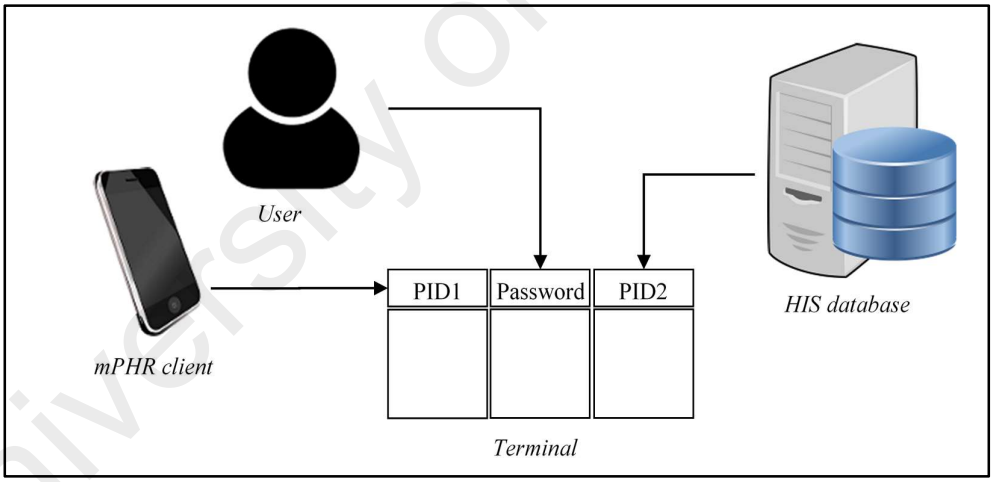


Figure 4.2: Patient authentication data within the terminal device

In Figure 4.2, the field ‘‘PID1” is the local patient identifier generated by each mPHR client. This identifier should be unique across all users visiting a certain terminal (potentially all users of the mPHR app nationwide) and can be made so by integrating parts of the user’s personal information into the generated identifier upon the creation of the personal health record on the mPHR client. The ‘‘Password” field is entered by the user of the mPHR client via the terminal interface each time the user asks to exchange

information with the HIS database at the other side of the terminal. On the first visit of the user, the terminal app generates a record for the new patient inside the database of the backend HIS application and creates an entry for the user in its own local authentication database. The created authentication entry stores the patient identifier received from the mPHR client in the ‘‘PID1” field, the password entered by the user in the ‘‘Password” field, and the generated patient identifier received from the HIS database in the ‘‘PID2” field.

Upon subsequent visits, the terminal uses the received identifier from the client to look up the correct entry of the user in the authentication table and then compares the stored password with the just-provided user password. If the comparison is positive, then the terminal uses the value stored in the ‘‘PID2” field to look up the correct record of the user in the HIS database. Thus, the terminal is effectively playing the role of a registration/authentication point for the visitors to the provider that the terminal serves. The functionality of the terminal is relatively analogous to the sign-up/ sign-in feature of web apps.

Addressing the issue of unique patient identifiers may raise the question of how to deal with the possible requirement for a national unique identifier. If national unique identifiers are already established, then the framework can adapt them without actually relying on their roles. A national identifier is only another piece of data that is attached to each personal record and can be reported with other information whenever necessary. However, the proposed framework has its own set of unique identifiers that are generated by the mPHR client and managed within the scope of the framework.

4.4.3 Health information system (HIS)

Health information system (HIS) refers to the main system that is running at the healthcare provider’s side which is responsible of capturing, storing, managing and

transmitting health related information including disease surveillance, laboratory, patient administration and human resource management information. Most of the healthcare providers do not allow third party agencies to access their own data even for research purposes. Fortunately there exists several health information systems that are open source and freely available to download. Such systems often comes with sample data sets to allow researchers and developers to conduct different kind of experiments. For the proposed framework, two open source HISs have been selected and adopted in order to complete the entire set of all required components. The selected Open Source Systems (OSS) are further described in more detail in Chapter 5.

4.5 Component interactions

The operation of the whole framework is divided into five distinct types of interactions. Each type dubbed with a three-letter acronym in the following listing.

4.5.1 User-Client Interaction (UCI)

Refers to the possible operations that the user can perform using the mPHR client application naturally, each type of operation would call for a separate “activity” or screen within the client app. Figure 4.3 describes those operations.

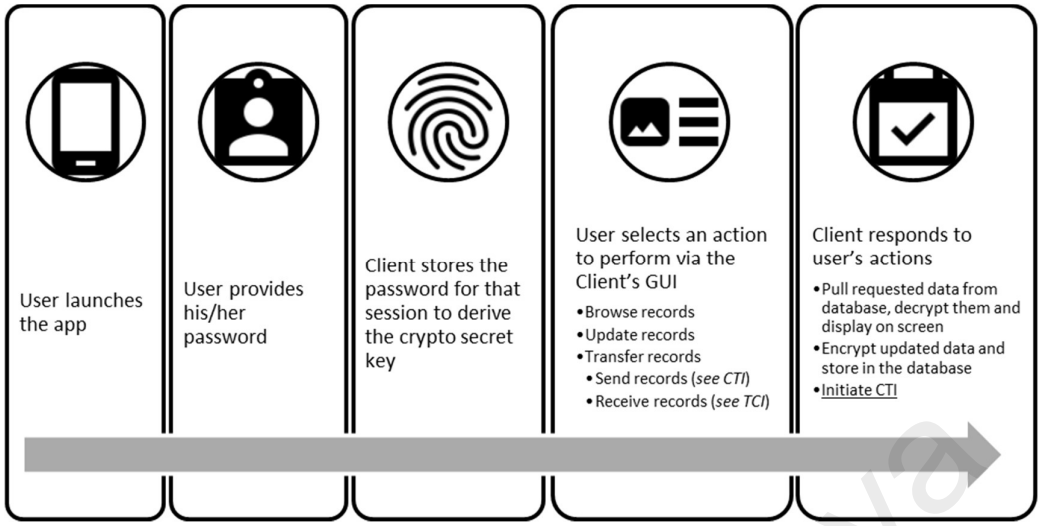


Figure 4.3: User-Client Interaction (UCI)

4.5.2 Client-Terminal Interaction (CTI)

Refers to the types of operations that involve the transfer of data in the direction from the client app to the terminal device. The client app allows the user to choose a partial set of his/her personal health records to transfer, and then decrypts the selected data for plain-text transmission. Other than that, this type of interaction between the client and terminal encompasses two important functions of the framework: the translation of the stored medical information into HL7 tags, and the exchange of the translated information over NFC connection. NFC is natively supported by the Android operating system, though as of this writing not all smartphone devices that run Android are NFC-enabled. Nevertheless, vendors of smartphones are increasingly adding NFC circuitry to their newer phones.

Using the API provided by Android, the developer of the app needs to write the code to wrap the exchanged data in NFC message and initiate as well as respond to data transmission at both ends in tandem with user taps. While writing the code, (Coskun et al., 2015) was mainly referred. While writing the code to process NFC messages and control their transmission, the official Android developers website was mainly referred

(Developers, 2016). Figure 4.4 illustrates the main steps in the interaction between the client and the terminal device.

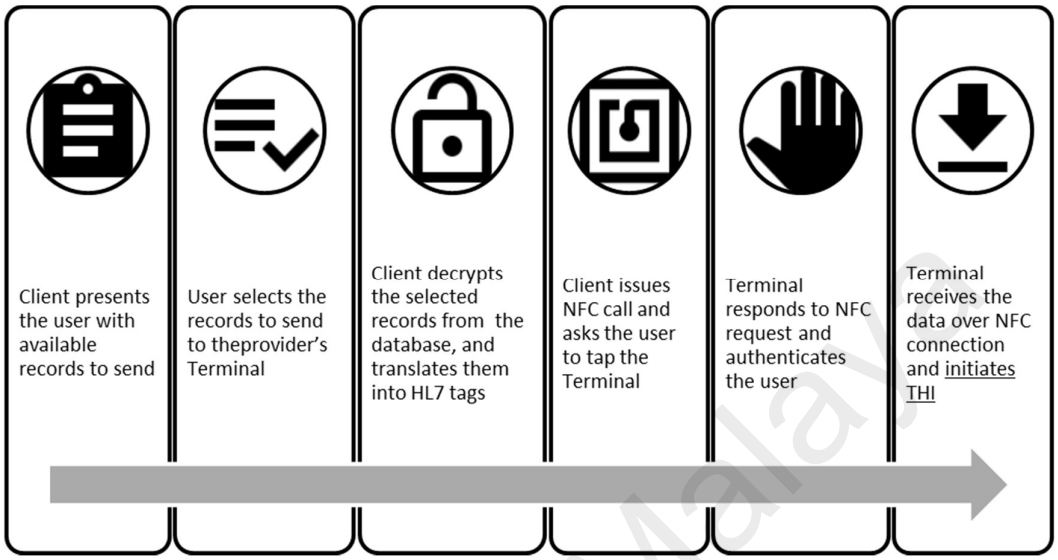


Figure 4.4: Client-Terminal Interaction (CTI)

4.5.3 Terminal-Client Interaction (TCI)

Refers to the types of operations that involve the transfer of data in the direction from the terminal device to the client app. This type of interaction is very similar to CTI above, and is detailed in Figure 4.5.

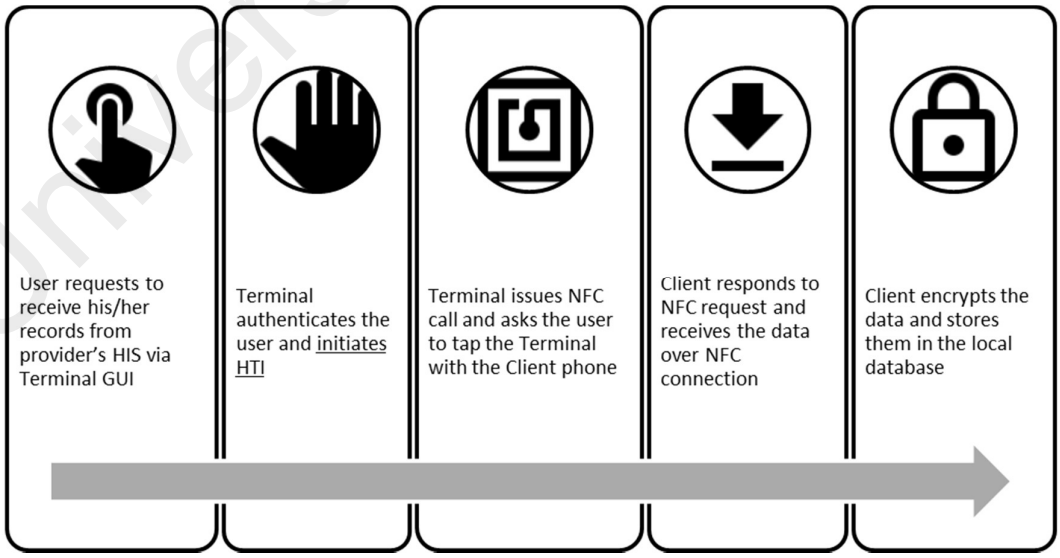


Figure 4.5: Terminal-Client Interaction (TCI)

4.5.4 Terminal-HIS Interaction (THI)

Refers to the types of operations that involve the transfer of data in the direction from the terminal to the provider's HIS database. As shown in Figure 4.6, this is a backend interaction within the premise of healthcare center and includes the key step of translating the received HL7-based messages from the clients into SQL statements that can duplicate the same information in the correct fields of the HIS database. For internal exchange of data between the terminal device and the HIS database, a secure Wi-Fi network that is not open for visitors is assumed to be available around.

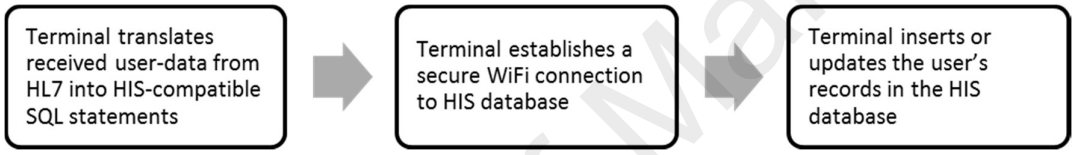


Figure 4.6: Terminal-HIS Interaction (THI)

4.5.5 HIS-Terminal Interaction (HTI)

Refers to the types of operations that involve the transfer of data in the direction from the provider's HIS database to the terminal device (Figure 4.7). Similar to THI above, this type of interaction occurs in the backend, implemented completely in code with no interface to the user.

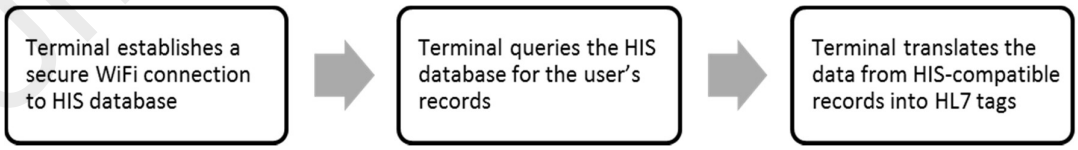


Figure 4.7: HIS-Terminal Interaction (HTI)

To put all these pieces in perspective, Figure 4.8 is drawn to show the overall operation flow between the client and terminal apps. It's notable that the last two backend interactions (THI and HTI) are not shown.

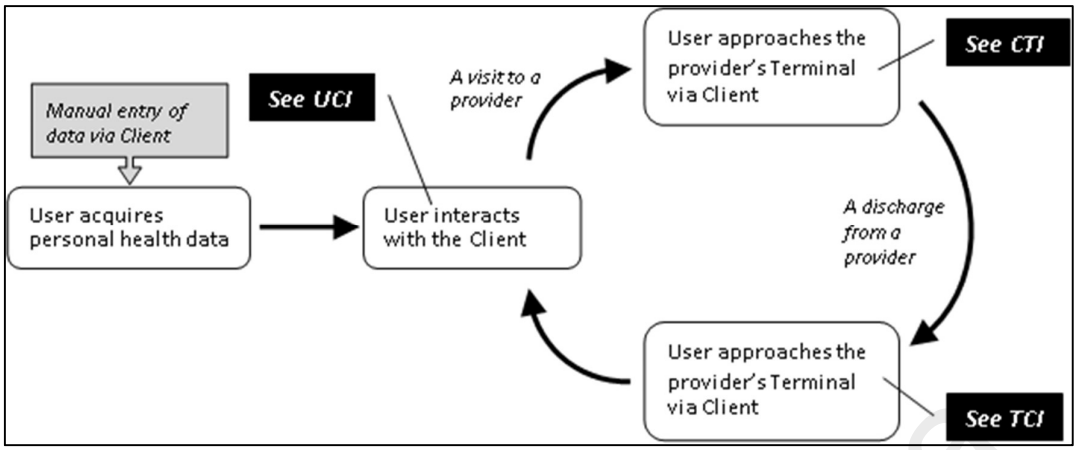


Figure 4.8: Overall operation of the framework

4.6 Chapter Summary

This chapter described the entire structure of the proposed framework along with its individual components. The chapter began with general overview of the proposed framework, followed by a detailed explanation of its interacting components, namely, the user's mPHR (client), provider's HIS (the server), and the interfacing device (the terminal). The content, purpose and features of each of these components were listed and explained in detail. Finally, the chapter was ended with flowchart illustrations that explain the flow of data during the interaction between the different components of the framework.

CHAPTER 5: FRAMEWORK IMPLEMENTATION

The aim of this chapter is to provide a proof-of-concept implementation for the proposed framework. The chapter starts by outlining few decisions that affected the prototype implementation. Subsequently, the process of implementing the different components of the proposed framework is described and the employed tools and technologies are listed. In particular, samples of the user interfaces for both client and terminal apps are provided and explained. For the server side, the two open source EMR systems that were employed to represent the provider's HIS are described. The chapter ends with a discussion of other implementation details pertaining to the implemented security and data-format options, followed by a brief summary.

5.1 Overall Implementation Decisions

The deployment of the proposed framework involves no changes to existing systems or infrastructure, and its implementation is possible using available commodity hardware and software technologies. In order to illustrate this fact and rudimentarily demonstrate the operation of the framework, an initial prototypic implementation has been built for the various framework's components described in the previous chapter. One important and recurrent strategy followed is to adopt open source technologies whenever possible, which further reduces the costs of implementing the proposed framework, among other benefits. For implementing the proof-of-concept prototype, the following design decisions have been made:

i. Open source technologies were adopted whenever possible:
    a) Android apps are built for mPHR client and the terminal components.
    b) OpenEMR and FreeMED are selected to represent HIS components.

ii. AES symmetric encryption with key password protection is chosen for the mPHR component.

iii. HAPI HL7 open source API for Java is adopted for mPHR client and the terminal components.

iv. Near Field Communication NFC for secure wireless connectivity option is employed for the mPHR client and the terminal.

5.2 Client and Terminal Apps Implementation

The main parts of the framework are essentially two apps, one for the mPHR client and another for the terminal device, with specific features that reflect the desired requirements of both components. Android operating system is chosen as the target mobile platform for both apps. Android is an open source platform that is originally intended for use in portable user devices (Arm, Misik, Bradac, & Kaczmarczyk, 2015). Android has a market share of more than 87% as of the second quarter in 2016 (IDC, 2016), which makes for an attractive platform for a nationwide-targeted application. Each app comprises a number of screens, called activities in the terminology of Android development. Those activities can be determined by referring to the flow of framework operations explained in Chapter 4 when discussing the components' interactions.

It is relatively straightforward to map the specified types of interactions into a set of Android activities. In Android language, an activity is a software module that has a user interface and corresponds to a single screen of an Android app. A single activity can wrap many functions that are initiated by the user input through the activity's interface, and need not be associated with a single type of interaction. For example, a button element for sending data on a client screen can execute several parts of the user-client interaction such as grabbing the data from the mPHR database, decrypting and translating them into HL7-based fields, as well as parts of the client-terminal interaction

such as wrapping the translated data in NFC messages and initiating the NFC connection. Before presenting the user interfaces for the client and terminal apps, the next subsection lists and briefly describes the tools used to build these apps.

5.2.1 Implementation Tools

As mentioned earlier, Android platform was adopted to implement the app components within the framework. Development for Android is supported by powerful and enterprise-level tools. Android apps are written in the Java programming language, which is also widely supported in all major operating systems. The most pertinent development tools are briefly listed below for a complete account on the implementation details.

(a) ***Android Studio***

Android Studio is the official Integrated Development Environment (IDE) supported by Google for Android app development. It provides the fastest set of tools for building apps on every type of Android device. It includes all common standard features such as code editing, debugging, performance profiling, and a flexible build/deploy system that allows the developers to focus on building high-quality apps. Other features offered by Android Studio include a fast and feature-rich emulator, a unified environment for all Android devices, the ability to make changes instantly to the running apps without building a new Android Package Kit (APK) file, code templates and GitHub integration, a comprehensive testing tools and built-in support for easy integration with Google cloud messaging and App Engine.

(b) ***Java Development Kit (JDK)***

JDK is the official development environment for building applications, applets, and components using the Java programming language. JDK contains the software and tools that are required to compile, debug, and run applets and applications written using the

Java programming language. JDK has a collection of programming tools, including *javac*, *jar*, and the *archiver*, which packages related class libraries into a single JAR file. This tool also helps manage many components together, including *jar* files, *Javadoc* (the documentation generator, which automatically generates documentation from source code comments), *jdb* (the debugger), *jps* (the process status tool, which displays process information for current Java processes) and *javap* (the class file disassembler).

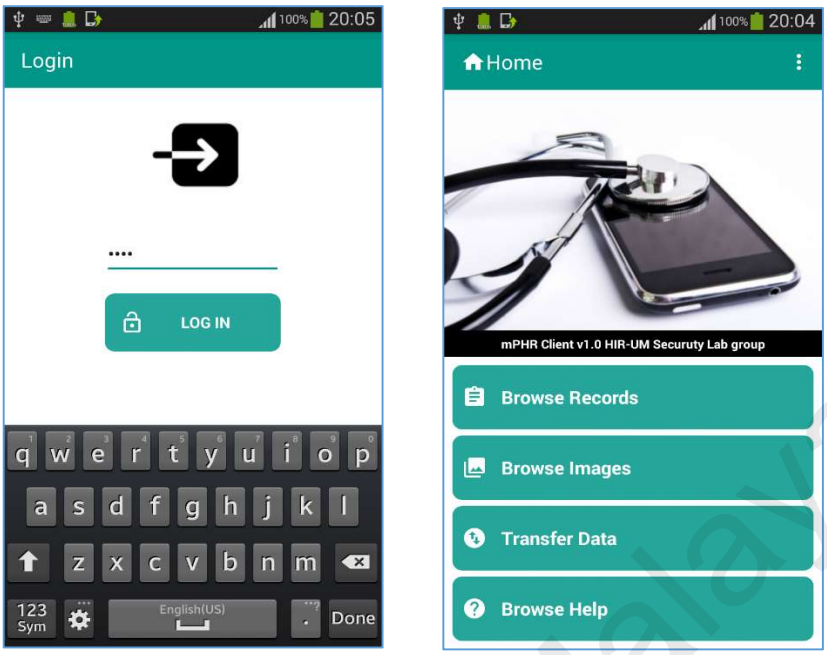
(c) ***Eclipse***

This is another IDE that is widely used for apps development. Eclipse is the most widely used Java IDE. It contains a base workspace and an extensible plug-in system for customizing the environment. Eclipse is written mostly in Java and its primary use is for developing Java applications.

5.2.2 mPHR Client Interface

This section presents and explains several screenshots of the client mPHR app. The app starts with the main login screen (Figure 5.1(a)), which is the first screen that appears when the app is activated. For the first time use, the patient will need to set a password. Later on, the correct password must be entered in order to be able to log successfully into the app. Once the user successfully logs in to the mPHR app, the first screen that appears is the home screen as shown in Figure 5.1(b).

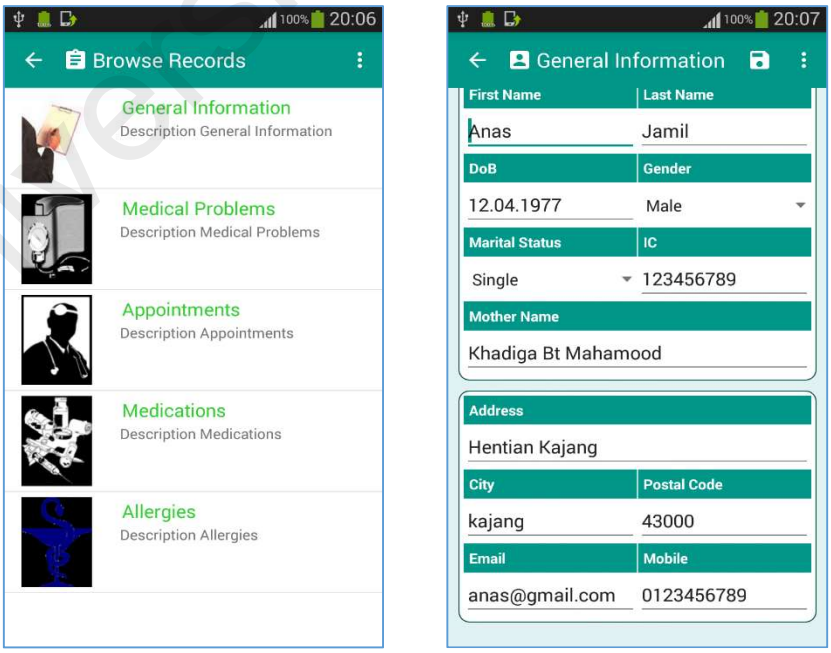
Initially there are four options available for the user to interact with the system. The first option "*Browse Records*" enables the user to view his/her health records which have been updated by the HIS. The second option "*Browse Images*" enables the user to view his/her medical related images including x-rays. The third option "*Transfer Data*" enables the user to transfer the data from the mPHR app to the HIS and vice versa, while the fourth option provides some kind of help to the user about the different activities that can be performed using this app.



(a) (b)

Figure 5.1: (a) mPHR login screen, (b) mPHR home screen

Once the user selects the first option "*Browse Records*", another screen appears with different options as shown in Figure 5.2(a).

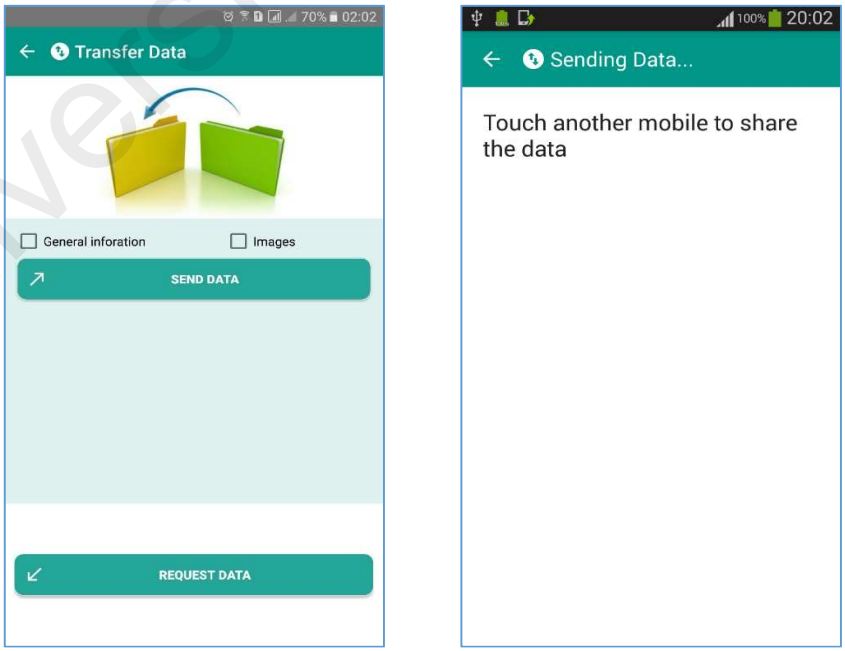


(a) (b)

Figure 5.2: (a) mPHR browse records screen, (b) mPHR general information screen

The "*Browse Record*" option leads in turn to several functions, such as "*General Information"*, which displays the patient's general information as seen in Figure 5.2(b), "*Medical Problems*", which displays the list of medical problems from which the patient suffers, "*Appointments*", which displays and notifies on a list of upcoming medical appointments, "*Medications*", which displays a list of medical prescriptions given by the physician, and "*Allergies*", which displays a list of allergy types from which the patient suffers and other information related to it, such as medicine or food types that cause these allergies.

Figure 5.3(a) shows the "*Data Transfer*" screen, which allows the user/patient to transfer or exchange his/her health records with other health providers through the terminal device. As observed in the figure, the data transfer function enables the user to select specific set of records to send to the health provider's terminal device upon clicking on the "*send data*" button. In the case of receiving data from the health provider, the user can request the transfer by clicking on the "*request data*" button.



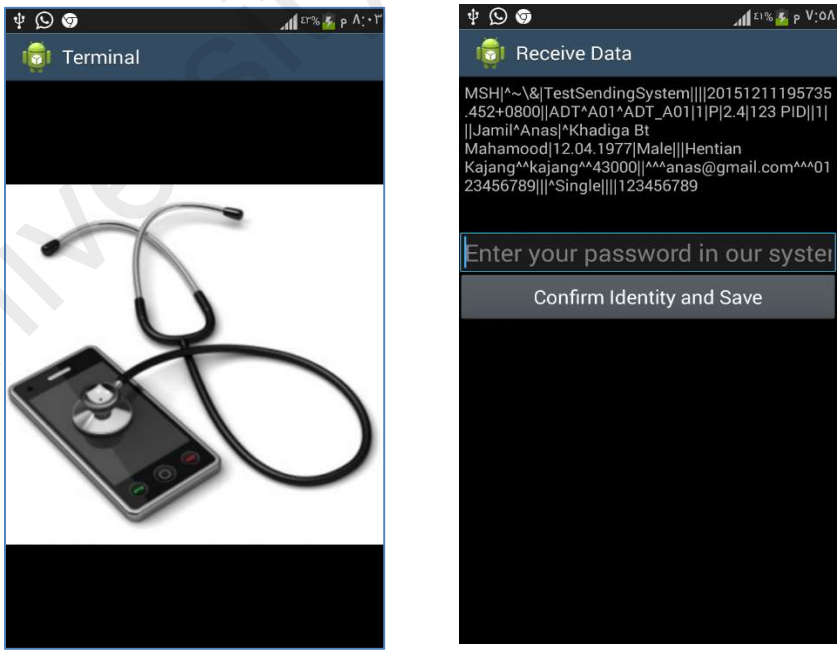
(a) (b)

Figure 5.3: (a) mPHR transfer data screen, (b) mPHR sending data screen

It should be noted that both devices (the mPHR client as well as the terminal device) must be placed very close to each other when transferring data, as required by the NFC technology used for data transmission. Figure 5.3(b) shows the next screen that appears when the "*send data*" button is pressed. As shown in the figure, the app will wait till the user appropriately touches the device with the other device (the terminal) in order to start the data transmission. As explained in the previous chapters, the distance between the two devices should be less than or equal to 10 centimeters.

5.2.3 Terminal Interface

This section presents and explains some screenshots from the terminal app. As discussed in the previous chapter, the terminal device is to be placed at the health provider's side. The main screen (Figure 5.4(a)) remains on and active all the time for the users. Unlike the client app, the user interface of the terminal's main activity is just a fixed image.



(a) (b)

Figure 5.4: (a) Terminal main screen, (b) Terminal authentication

Most of the terminal's interactions with the client on one hand and with the HIS database on the other hand need no direct input from the user except when authenticating the user using a simple password, as presented in Figure 5.4(b). Once the patient places his/her mPHR close to the terminal device and initiates the data transfer, the patient ID is automatically fetched out and the terminal device will ask the patient to enter the password for authentication. Figure 5.4(b) also displays the received message to showcase the HL7-based content of the exchanged information.

5.3 Health Provider's HIS

The last part of the framework is the traditional health information systems owned and operated by healthcare providers. In general, every provider employs a different, proprietary HIS that is not open to access for experimentation. Fortunately, there exist a set of open source EHR systems that are deployed by many healthcare providers. A few of these applications are discussed and compared in (Kiah, Haiqi, Zaidan, & Zaidan, 2014). While selecting the HIS in order to integrate and test the implemented framework apps, several points have been considered, such as whether the HIS is open source, mature, freely available and highly adopted in several hospitals.

In the initial experimentations, two systems were adopted, the OpenEMR project (OpenEMR, 2016) and FreeMED (FreeMED, 2017). As those systems are web-based applications, a local web server was setup to run the application on traditional PCs and connect the terminal device to its database through local and secure Wi-Fi network. OpenEMR and FreeMED played the role of HIS applications in this way, while mPHR client apps were installed on a few devices and utilized terminal apps to connect to the open source EMR applications. The required translation was developed between HL7-based fields and the fields of the EMR databases for selected tables, and embedded that in the terminal apps. This process of building special terminal apps for each HIS

database is required at every provider's location, as discussed earlier. Following subsections describes the OpenEMR and FreeMED health information systems as well as the local web server used to run the system on a traditional PC.

5.3.1 OpenEMR

OpenEMR is a free and open source electronic health records and medical practice management application. It is certified by the Office of the National Coordinator for Health Information Technology (ONC) and it features fully integrated electronic health records, practice management, scheduling, electronic billing, internationalization, free customer support, and a vibrant community (Donahue, 2009). It runs on Windows, Linux, Mac OS X, and other platforms and is released under the GNU General Public License. Figure 5.5 displays the login screen for OpenEMR.

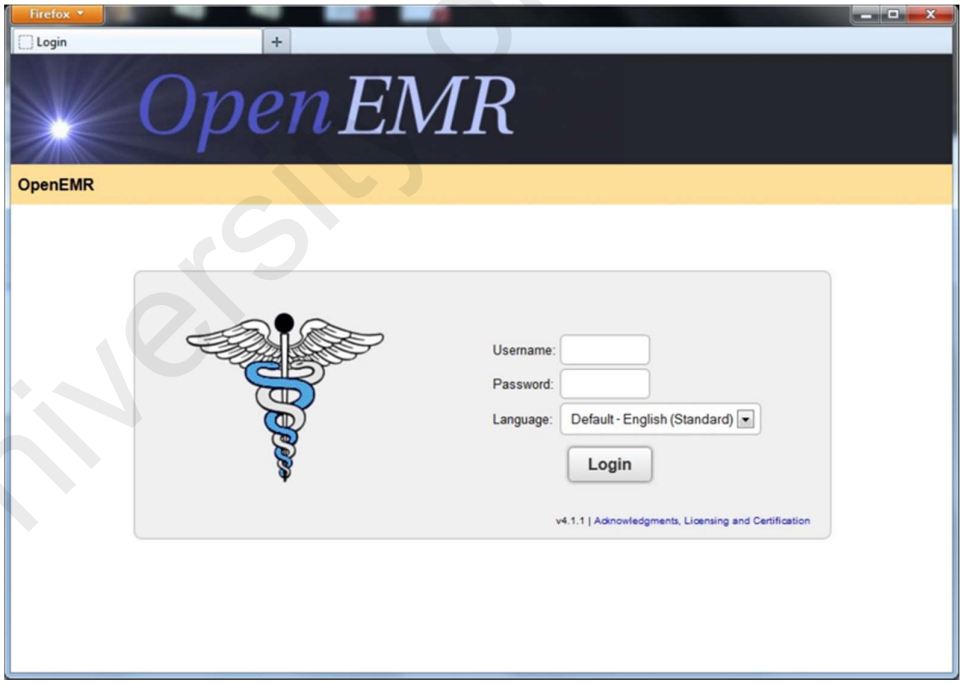


Figure 5.5: Login screen for OpenEMR

The OpenEMR patient demographics consist of primary information (name, date of birth, sex, and identification), marital status, contact information of patient and patient's employer, primary provider, HIPAA information, language, ethnicity and insurance

coverage. Patient scheduling includes patient appointment notification via email and SMS, compact and flexible appointment calendar, which includes features like finding appointment slots, categories for appointment types and repeating appointments. The electronic medical records include encounters, medical issues, medications, immunizations, vitals, forms and clinical notes, labs, procedures, patient reports, patient notes, disclosures, clinic messaging, dated reminders, prescriptions and tracking patient prescriptions and medications. Figure 5.6 shows OpenEMR patient summary which includes most of the information mentioned above.

Figure 5.6: OpenEMR patient summary

5.3.2 FreeMED

FreeMED is an electronic medical record and practice management system for medical providers. It is GPL-licensed and has been developed since 1999 (Kobayashi, 2012). It provides an XML-RPC backend and multiple import and export formats, as well as reporting and other features. The main programming language used to write FreeMED is PHP, and it makes heavy use of SQL, favoring the MySQL database

engine. It also uses some bash, Perl, and small pieces written in other languages. Its interface is primarily web-based, but web services interfaces, such as XML-RPC, are also available. Figure 5.7 shows the login screen of FreeMED, while Figure 5.8 shows FreeMED home screen after successfully logging in.

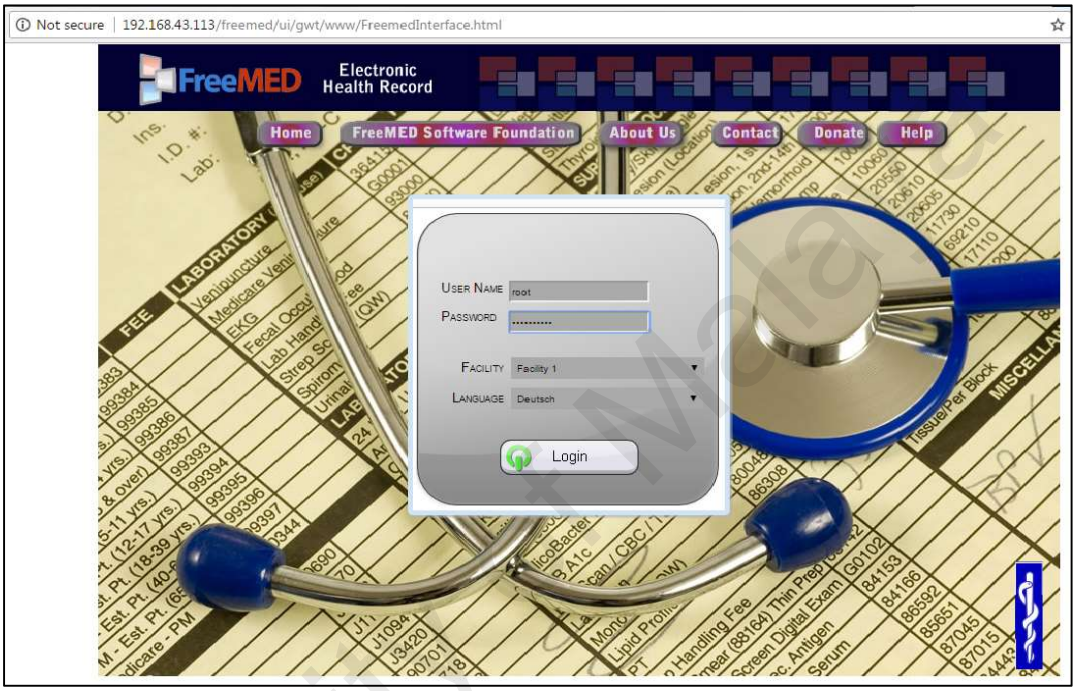


Figure 5.7: Login screen for FreeMED

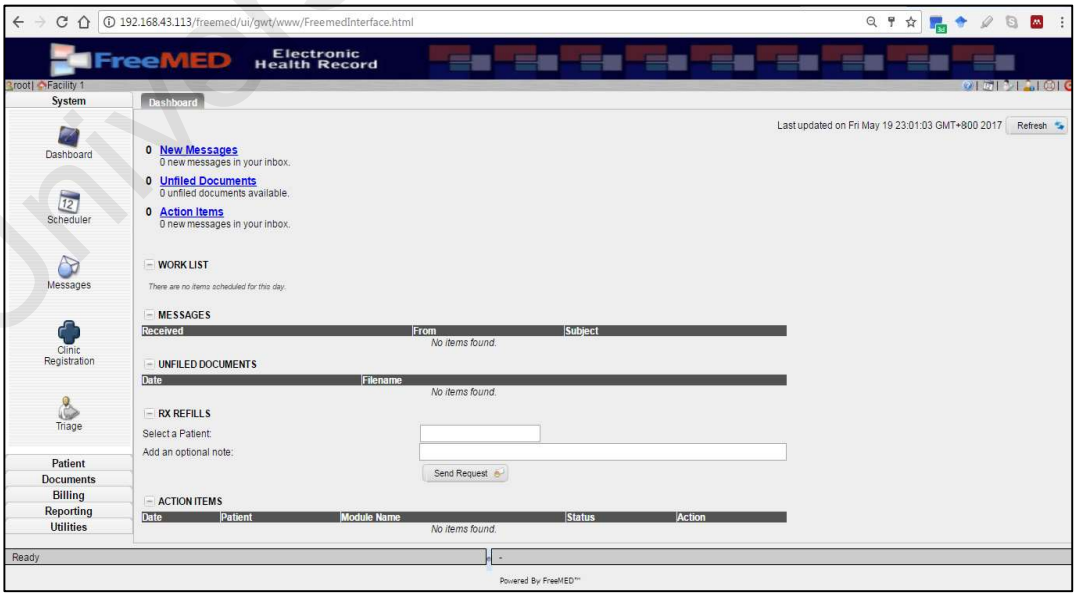


Figure 5.8: FreeMED home screen

5.3.3 WampServer

WampServer is a Windows-based web development environment which allows creating web applications with Apache2 web server, PHP scripting language and a MySQL database. WampServer's functionalities are complete for developing and running web applications on local servers. Once the WampServer is running, the localhost page can be accessed through any web browser and the following WampServer's start screen appears as shown in Figure 5.9. In this case, OpenEMR project is already hosted on WampServer and hence it can be accessed by clicking the following link http://localhost/openemr/interface/login/login_frame.php?site=default.

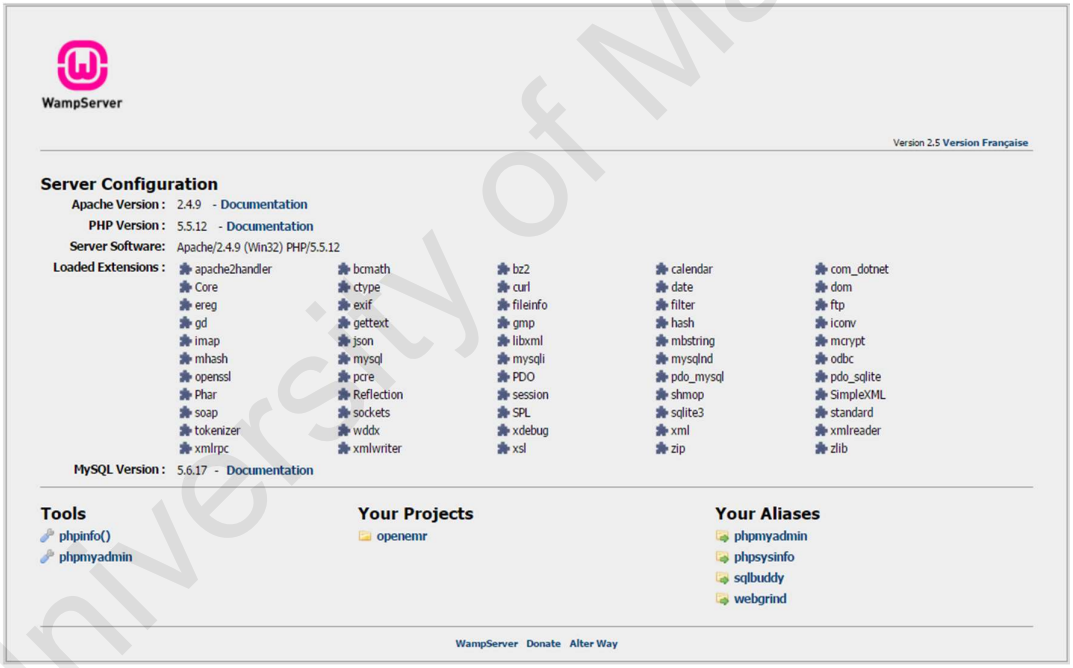


Figure 5.9: WampServer localhost start screen

5.4 Other Implementation Details

There are other points related to the initial implementation of the apps that are missing from the above discussion, these points are briefly discussed in this section.

5.4.1 Encryption standards

It was previously required that the data be encrypted within the mPHR app in order to maintain the data secrecy and confidentially if the device is lost or stolen. A symmetric key encryption scheme has been adopted to achieve this requirement. Since one key will be used for encryption and decryption, drawbacks of maintaining the keys are eliminated. A password-based encryption is used, in which the encryption key is derived or generated based on the password entered by the user. Expectedly, from the many symmetric key encryption algorithms, the popular Advanced Encryption Standard (AES) (Daemen & Rijmen, 2013) was used to cipher the data inside the mPHR local database.

Implementations of the AES algorithm are widely available in software libraries, including libraries of the Java language, which is used in development for the Android platform. The actual code employed to implement password-based encryption on Android can be found in (Elenkov, 2012). For demonstration purposes, Figure 5.10 illustrates a snapshot of the development environment, showing how encrypted data appear in the mPHR database in the lower part of the figure.

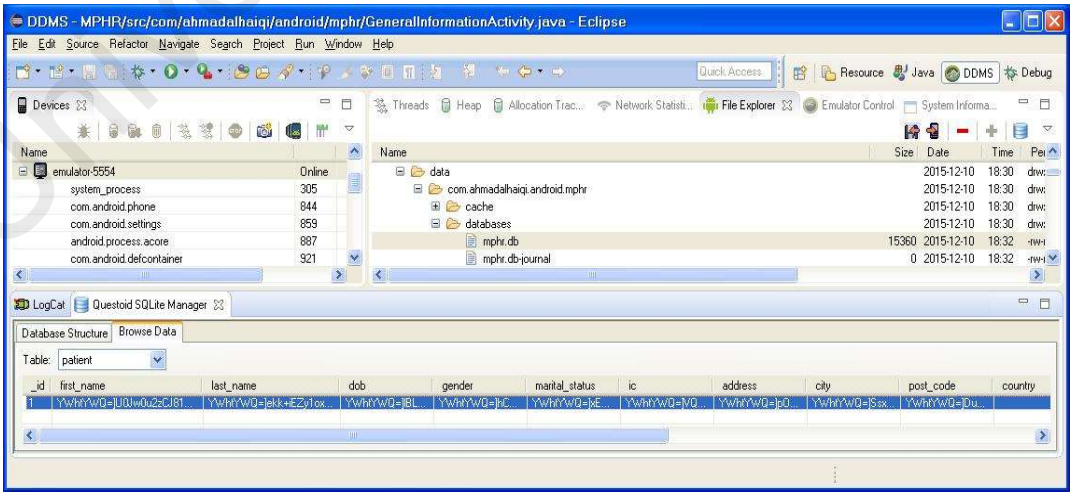


Figure 5.10: Encrypted record inside the mPHR database

5.4.2 Password hashing

One of the most basic security considerations while designing any application that accepts a password from users is hashing the password. Hashing protects the stored password in the local database from being stolen in case the database is compromised. This protects not only the user application, but also the accounts of the user on other services, if the same password is used. For this purpose SHA-1 hashing algorithm is applied to the user's password before storing it in the local database of the mPHR app. It shall be noted that the SHA-1 hashing algorithm has been also used along with other randomly generated number called 'salt' in deriving the encryption key as mentioned earlier for the symmetric key encryption (Elenkov, 2012), which ensures that the encryption key is both sufficiently random and hard to brute force.

5.4.3 HL7 message standard

Another point to be highlighted is the implementation of the translation to and from HL7 format. To achieve this, an open source API called HAPI (HL7 Application Programming Interface) (HAPI, 2016), which is a Java-based parser for HL7 messages, was adopted.

5.4.4 Patient Unique Identifier (PID)

The proposed framework design requires a unique identifier number to be generated for the mPHR app in order to identify each patient uniquely with all visited health providers. This requirement has been taken care of during the implementation stage of the mPHR app by assigning a unique number generated based on the combination of either identity card (IC) or passport number and date of birth of the patient.

5.5 Chapter Summary

This chapter presented and described the prototypic implementation of the proposed framework. Based on the hardware and software requirements established for each

component in the previous chapter, this chapter discussed the selections made in terms of technologies and tools to realize the proof-of-concept implementation of the two main components (the mPHR client, and the terminal). A number of screenshots showed the individual components in action. Finally, the selection of the open source health records systems that have been used to implement the proposed solution along with their enabling technologies was presented.

CHAPTER 6: PROTOTYPE VALIDATION AND DISCUSSION

The focus of this chapter is on the test and validation of the proposed and implemented framework. The key features and main functions of the implemented framework are tested against the specified requirements. A validation scenario has been described and accordingly different kind of tests were conducted in order to ensure that the prototype implementation is functional and meeting the specified requirements.

6.1 Validation Scenario

The implementation described in chapter 5 is only meant to serve as a proof-of-concept to validate the idea of the framework. That is, the purpose of the prototype is to show whether, and how, the various components as well as their operations might be realized. To illustrate the result of this work further, the following subsection describes a simple test scenario to validate the different requirements set forth in Chapter 4. Along each step of the test, a screenshot is provided either from the client mPHR, the terminal device, or the utilized open source EMR. Table 6.1 lists the steps of the scenario.

The stipulated scenario assumes that hospital 'Putrajaya' is running OpenEMR as its hospital information system and it has previously developed a terminal app on a smartphone or a tablet. Similarly, it is assumed that hospital 'Serdang' is running FreeMED as its hospital information system and it runs its own terminal app on a smartphone or a tablet. The terminal devices are connected to the respective health information systems and have access to predefined and specific information of the patients. On the other hand, it is assumed that a patient is owning a smartphone and has installed the mPHR application on the phone.

Table 6.1: Validation Scenario

OpenEMR	FreeMED
New Visit The patient visits the Putrajaya hospital, and the hospital acquires the patients' record for the first time. The terminal inserts the record into the OpenEMR system used by the hospital (Figures 6.1, 6.2, 6.3 and 6.4).	
Discharge Patient updates own record from the hospital's OpenEMR system. A future visit appointment is also given to the patient (Figures 6.5, 6.6 and 6.7).	
	New Visit Patient visits Serdang hospital for the first time and the hospital acquires patient's record into its own FreeMED EMR system (Figures 6.8, 6.9, 6.10 and 6.11).
	Data Update Patient notices that the address field has not been changed to reflect the recent move from Block C 324 Jalan Tenaga 3 to A-123 South City. The address is updated within the hospital's EMR system (Figures 6.12 and 6.13).
	Discharge A visit is scheduled for the patient two days ahead, and the patient updates own records upon leaving the hospital (Figures 6.14, 6.15, 6.16 and 6.17).
Revisit Patient visits the Putrajaya hospital on the appointed date and transfers own record to the hospital's OpenEMR system along with the updated address (Figure 6.18).	

The steps in Table 6.1 covers the following main operations:

- Registering a new patient at each terminal device.
- Adding a new record to the provider's EMR system from the client mPHR.
- Transferring the data back with updates from the provider's EMR system to the client mPHR.
- Updating an existing record in the provider's EMR from the client mPHR.

The steps of the described scenario in Table 6.1 are further elaborated below.

(a) New Visit to Putrajaya Hospital

The patient visits the Putrajaya hospital, and the hospital acquires the patients' record for the first time. The terminal inserts the record into the OpenEMR system used by the hospital. In the simulated scenario, a patient named *Fadilha Saber* is visiting the Putrajaya hospital for the first time. OpenEMR system is being used by this hospital. Figures 6.1 and 6.2 shows first the existing records in the system and its internal database before the patient's visit to the hospital.

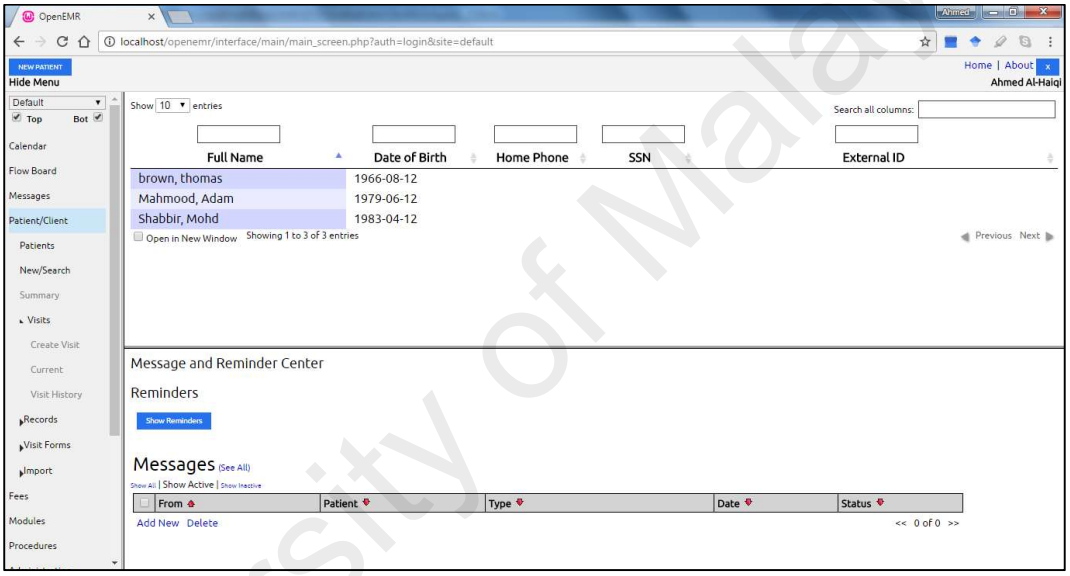


Figure 6.1: Snapshot of OpenEMR system before acquiring the patient's record

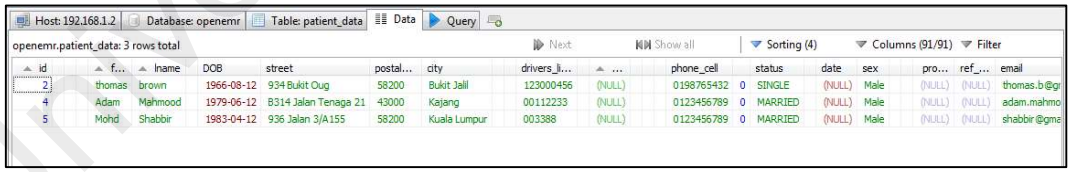


Figure 6.2: Snapshot of internal database of OpenEMR before acquiring the patient's record

After the hospital acquires the patient's data, her record is added to the OpenEMR system and its internal database, as shown in Figures 6.3 and 6.4.

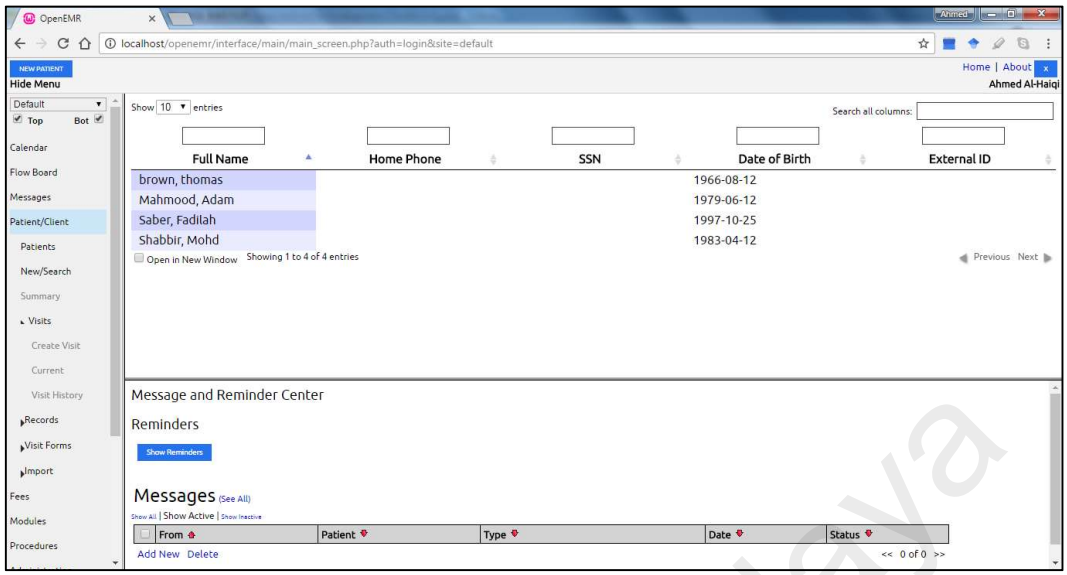


Figure 6.3: Snapshot of OpenEMR after acquiring the patient's record

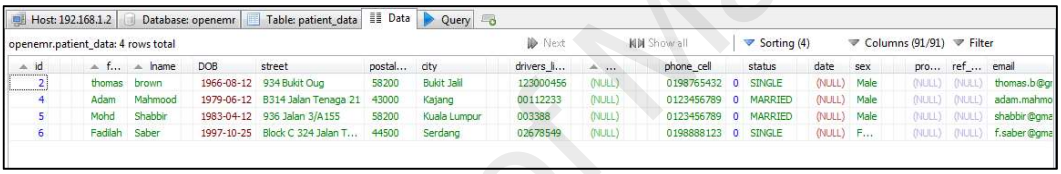


Figure 6.4: Snapshot of OpenEMR internal database after acquiring the patient's record

(b) ***Discharge***

Upon patient discharge from Putrajaya hospital, the patient updates her own record from the hospital's OpenEMR system via the terminal device. The patient also receives an appointment for a future visit. Figures 6.5 and 6.6 depict the appointment details in the OpenEMR system and its internal database after scheduling an appointment.

Figure 6.7(a) displays the mPHR application at the time when data are received from the hospital terminal. It shows the Health Level 7 (HL7) format in which data are received. Once data are received, a message appears on the mPHR screen stating that *Data Encrypted and saved successfully*. As mentioned earlier, data are encrypted inside the mPHR database to ensure secrecy. Figure 6.7(b) shows the appointments that is being added into the mPHR app.

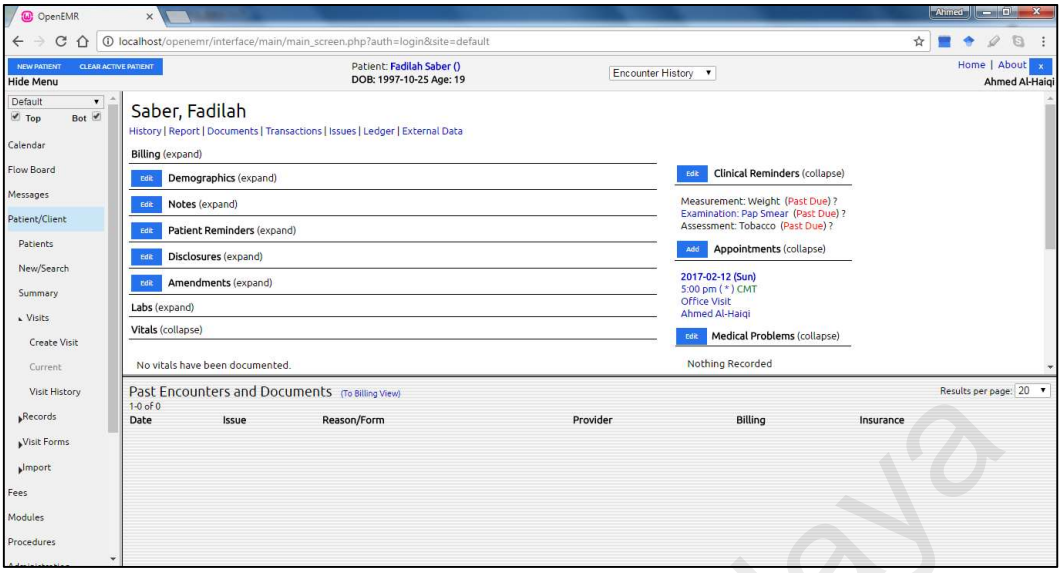
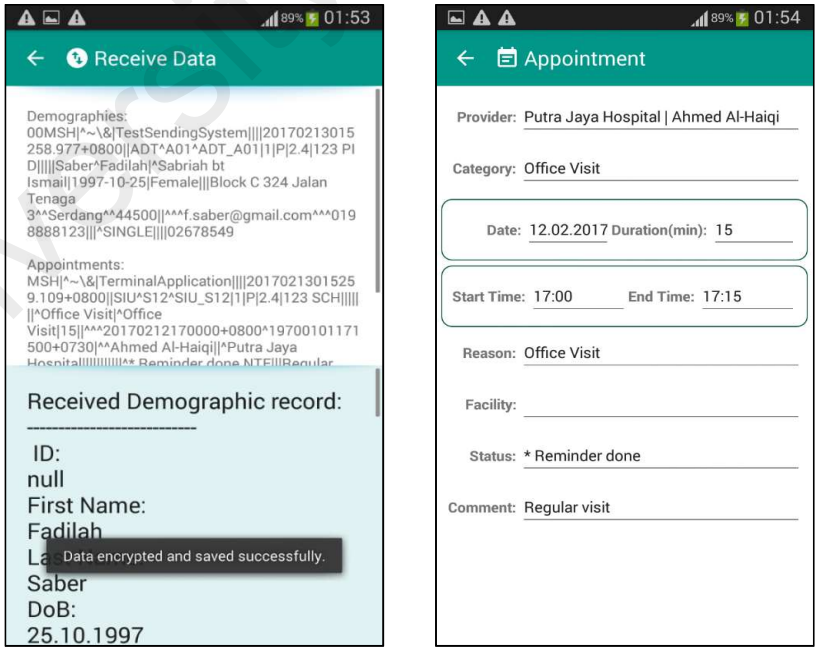


Figure 6.5: Snapshot of OpenEMR system after scheduling an appointment

Figure 6.6: Snapshot of OpenEMR internal database after scheduling an appointment



(a) (b)

Figure 6.7: (a) Snapshot of mPHR client after receiving the record from OpenEMR, (b) Snapshot of mPHR client appointment

(c) New Visit to Serdang Hospital

According to the described scenario, the patient *Fadilah Saber* decides to visit Serdang hospital for the first time. The EMR used by this hospital is FreeMED, and it also uses a terminal device to interface with patients' mPHR apps. Once the patient arrives at Serdang hospital, she transfers her personnel health record to FreeMED using the terminal interface, and the hospital acquires the record. Figures 6.8 and 6.9 shows the existing records in the FreeMED system and its internal database before the patient has performed the visit to the hospital.

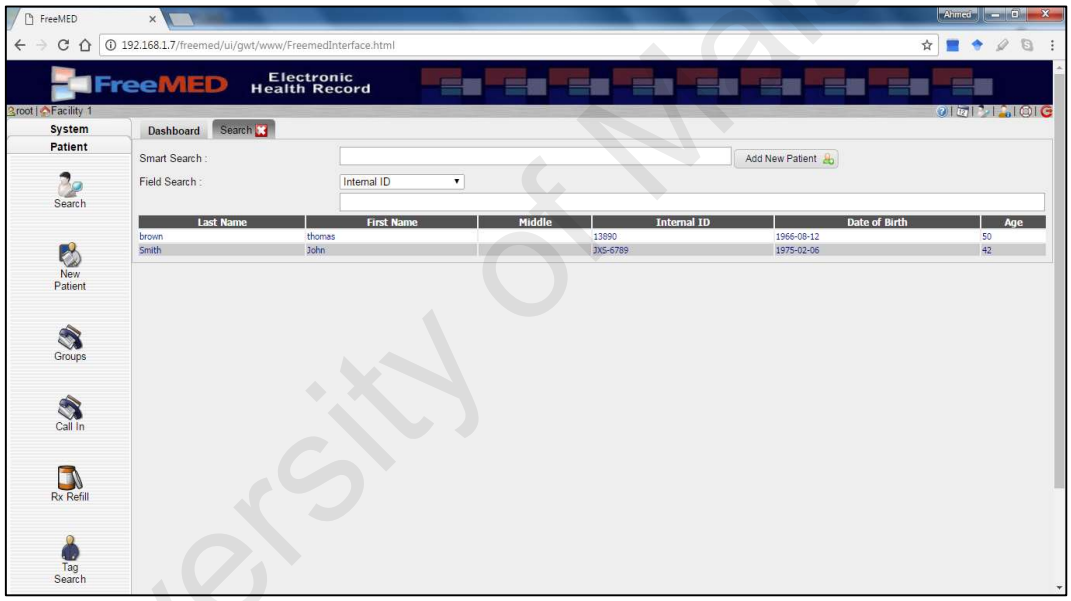


Figure 6.8: Snapshot of FreeMED system before acquiring the patient's record

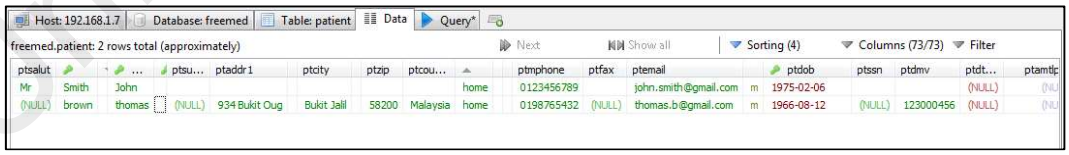


Figure 6.9: Snapshot of FreeMED internal database before acquiring the patient's record

After the hospital acquires the patient's data, a new record is added to the FreeMED system and its internal database as shown in Figures 6.10 and 6.11.

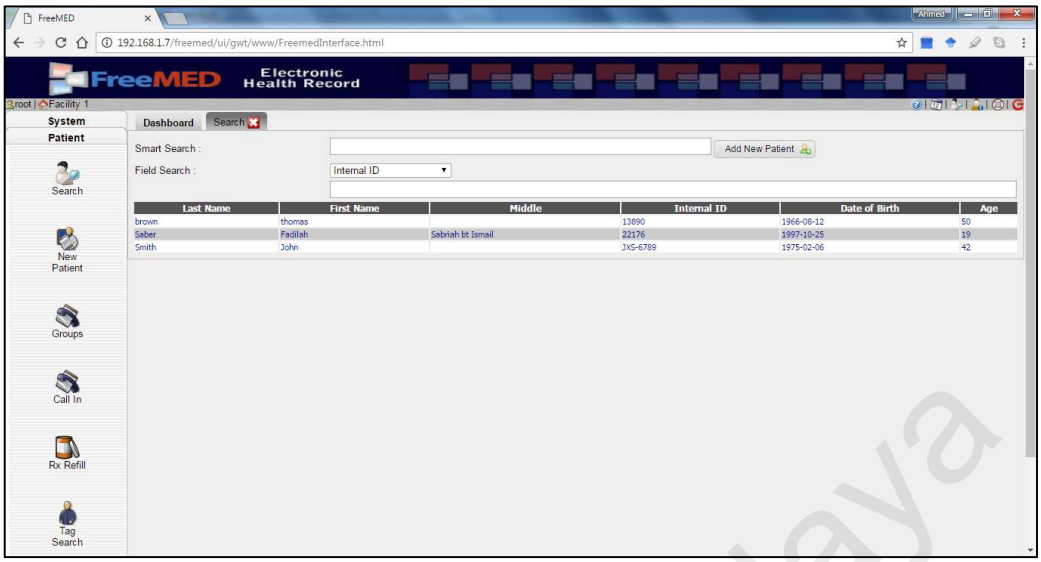


Figure 6.10: Snapshot of FreeMED system after acquiring the patient's record

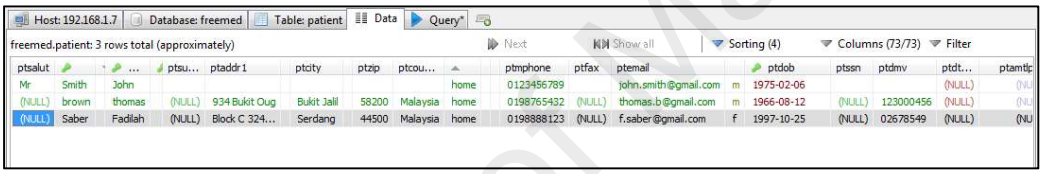


Figure 6.11: Snapshot of FreeMED internal database after acquiring the patient's record

*(d) **Data Update***

Continuing the presumed scenario, the patient notices that the address field has not been changed to reflect the recent move from Block C 324 Jalan Tenaga 3 to A-123 South City. Therefore, the patient decides to update the address while at the Serdang hospital, and the update is first made in the hospital's EMR system. Figures 6.12 and 6.13 are snapshots taken from FreeMED system while updating the patient's address and after the records are stored in the database, respectively.

Upon patient discharge from Serdang hospital, the patient updates her own mPHR record from the hospital's system. The patient also receives an appointment for a future

visit. Figures 6.14 and 6.15 depicts the appointment details in the FreeMED system and its internal database after scheduling an appointment.

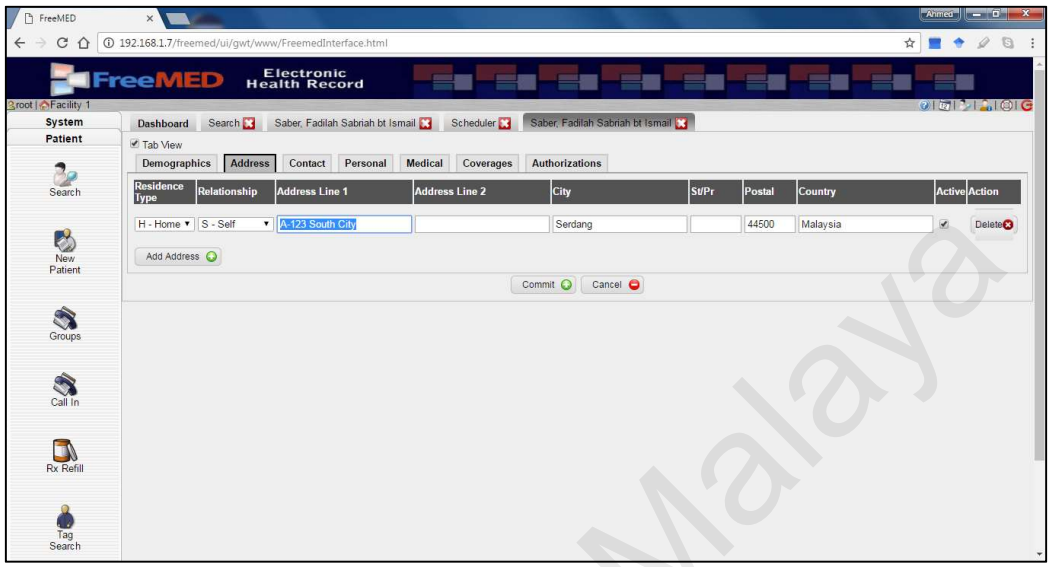
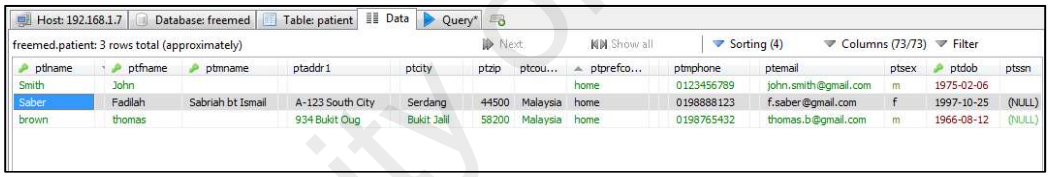
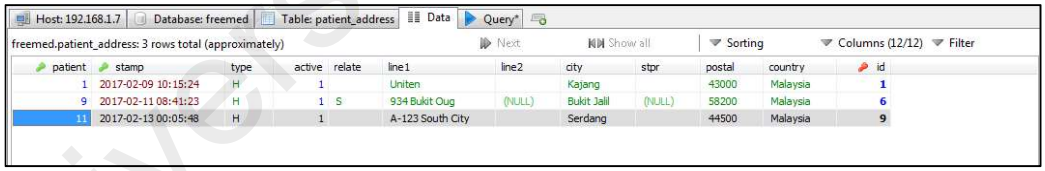


Figure 6.12: Snapshot of FreeMED while updating the patient's address



(a)



(b)

Figure 6.13: Snapshot of FreeMED internal database after updating the patient's address (a) in the patient table, and (b) in the address table

Figure 6.16 displays the hospital terminal application at the time when data are sent from the hospital terminal to the patient's mPHR. It shows the Health Level 7 (HL7) format in which data are sent from the terminal device. After the client is verified and data are ready for transmission, the terminal device notifies the client to touch the device in order to receive data

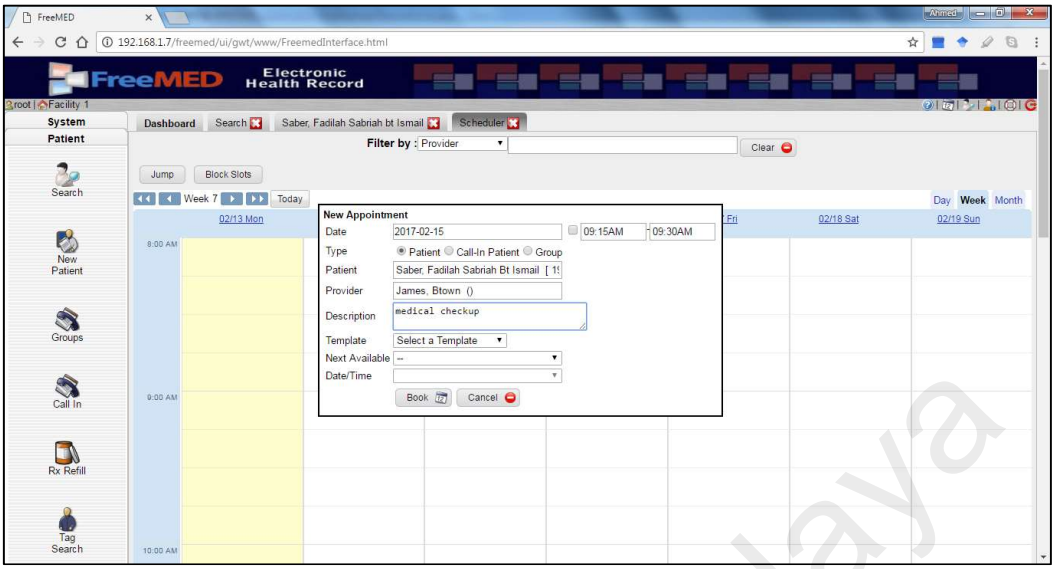


Figure 6.14: Snapshot of FreeMED system while scheduling an appointment

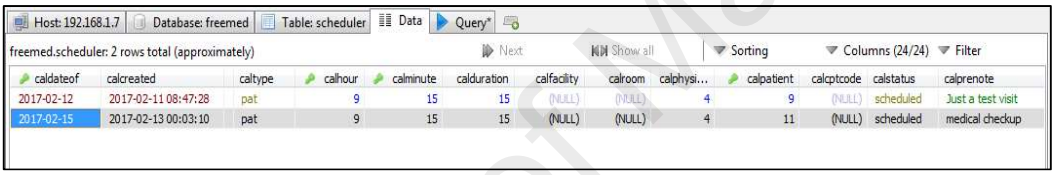


Figure 6.15: Snapshot of FreeMED internal database after scheduling an appointment

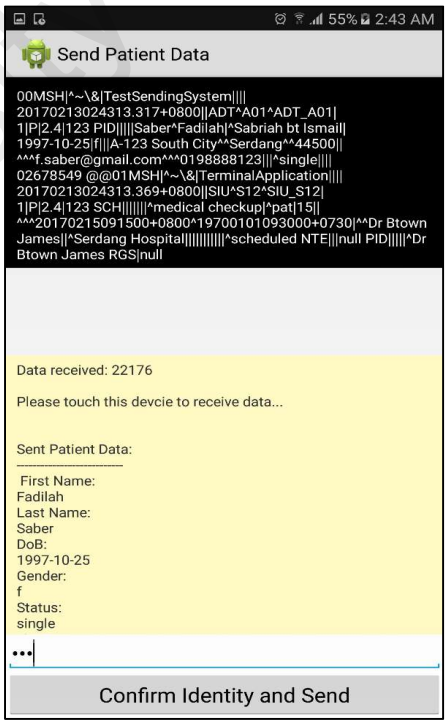
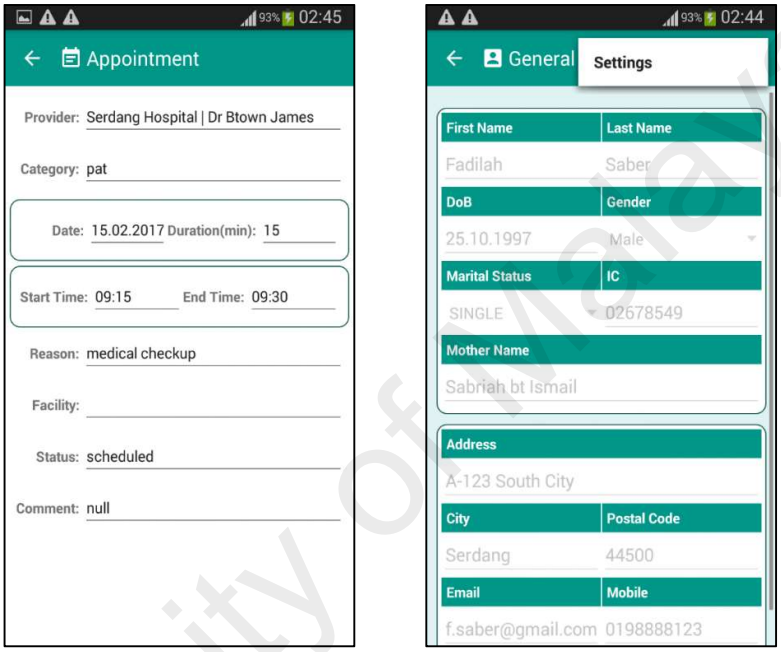


Figure 6.16: Snapshot of the terminal device sending data from FreeMED to the client

After the client receives the updated records from the hospital terminal device, the records are saved in the local mPHR database in encrypted format. Figure 6.17 depicts the updated client mPHR app after data have been received from the FreeMED terminal device. The figure shows the new appointment (Figure 6.17(a)) and the updated patient information, where the address has been updated to A-123 South city (Figure 6.17(b)).



(a) (b)

Figure 6.17: Snapshot of the updated patient after receiving the data from the FreeMED terminal device (a) the new appointment, (b) updated address

(e) ***Revisit***

The final test of this validation scenario assumes that the patient visits the Putrajaya hospital again on the appointed date, and transfers her personal record to the hospital's OpenEMR system (including the updated address). Figure 6.18 depicts the updated database in OpenEMR after acquiring the patient's details with the updated address.

The described simulated scenario has shown that the patient is capable of interacting and exchanging information with two different hospitals running on two different HISs.

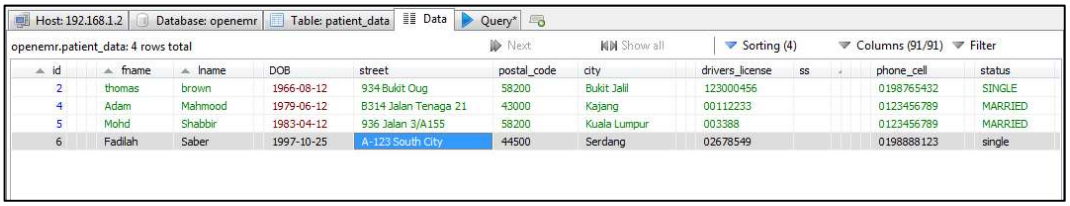


Figure 6.18: Snapshot of the updated OpenEMR database after receiving the data from the patient mPHR

Throughout those different operations, the following key requirements have been validated:

- Proper protection to the data inside the mPHR database through encryption.
- Successful connection between the client devices and terminals through NFC in both directions.
- Successful connection between terminals and the EMR systems through secured Wi-Fi networks.
- Successful authentication of patients by the terminals at each visit after the initial registration upon the very first visit.
- Mapping health data in both the mPHR and the EMR databases to HL7 fields. Each datum in the mPHR database is correctly moved to the corresponding field in the EMR database by being translated first to the right HL7 field and then from the latter to the appropriate SQL statement that moves it into the EMR database. Both the mPHR client and the terminal understand HL7 but neither understands any of the other's format.

In the following section some highlights related to the above scenario are discussed in more details

6.2 Discussion

It should be noted that the mapping of health data from mPHR to HIS in the prototypic implementation covered only a very small portion of the EMR database, including samples of patients' data such as basic demographics and sample encounter management data such as appointment scheduling. Those samples, however, are quite representative of the principle of mapping data to and from the HL7 format. Covering the complete EMR database (a task that is expected from each provider in the proposed framework) becomes a matter of studying the relevant parts of the HL7 specifications and having a good documentation for the database itself. After that, the process is a (tedious) programming exercise of reading the data from the correct field(s) of the HL7 messages sent by the client, then writing those data into the correct table(s) of the EMR database, and vice versa.

In the case of implementing the terminal as an Android smartphone or tablet, that programming exercise will be done in Java, which has a very good support for communicating with various databases, including those powered by the popular MySQL database management system. Moreover, the Java-based HAPI HL7 parser can be used, which significantly simplifies the extraction of data from HL7 messages, as well as wrapping data into HL7 messages.

The relevant parts of the HL7 specification that should be studied and implemented by the terminal lie at the intersection of two parts of the standard: the one that covers all health information in the HIS associated with the terminal, and the one that encompasses all personal health information within the client mPHR. The scope of the former is well known for the HIS providers separately, each for its own system, while the latter is public by design, and should be learnt by every provider in order to plug into the framework. In this sense, the (sub)-set of HL7 messages that can be produced

and consumed by the client mPHR resembles the operating systems' public APIs that are known to peripheral manufacturers, and for which they write their device drivers. Similarly, healthcare providers write their terminal apps to translate between their own data format and the set of HL7 messages supported by the mPHR client.

At this point, it is assumed that the mPHR client covers an adequately comprehensive set of HL7 messages to cover the expected functionality of an mPHR, which should include all data of direct interest and relevance to the consumer itself, rather than the provider (such as data on aspects of practice management). However, the exact content of the mPHR client remains an open issue, and its definition largely relies on the entity that will endorse the first implementations of the mPHR client. Such definition can be based on existing standardization efforts for PHRs; e.g., HL7 Personal Health Record System Functional Model (PHR-S FM) (HL7, 2017b), though this model explicitly excludes message and record specifications from its scope (Mon, Ritter, Spears, & Van Dyke, 2008). In any case, adding support for additional HL7 areas is incremental, and hence can be added on in later stages to either the mPHR specification or the terminal mappings with no radical change to the present implementation.

Talking about HL7 implementation to achieve interoperability, one point to emphasize here is that the interoperability model is different from the model of many initiatives and projects that attempted to tackle this challenging task e.g. (Rea et al., 2012; Sun et al., 2015). In this framework, the problem of interoperability is shifted from one between indefinite number of HIS sources into one between just two formats. The mPHR client app is expected to adhere to HL7 format, and so is each provider through its terminal app. No one is asked to integrate or even know about any data format other than its own and the corresponding HL7 parts of the HL7 standard. The

domain of conflicts is much less now, and the mapping process can be performed using the computational capability of current smartphone devices.

One question is left, however, which is whether the HL7 standard itself is adequate to cover all healthcare-delivery needs. It is assumed here that HL7 is comprehensive enough as any international standard should be, and leave the question for standardization organizations to answer. After all, the framework can replace the unified format with any feasible custom format, but the benefit of all standardization heritage and future will be lost, and yet, the produced custom format would still be susceptible to the same questions about comprehensiveness.

6.3 Chapter Summary

This chapter validated the key features and main functions of the implemented framework to ensure that it satisfies the specified requirements in previous chapters. A simulation-based validation scenario has been described in which few test cases were conducted in order to validate the functionality and features of the prototype implementation such as the interoperability, data transfer, data storage and security. All tests were successful and demonstrated that the proposed framework including its three main components (the mPHR, the terminal device and the HIS) can provide the required level of interoperability and connectivity between healthcare providers and hence achieving the desired health information exchange.

CHAPTER 7: CONCLUSIONS AND FUTURE WORK

The aim of this chapter is to provide an overall conclusion to the research work in this thesis. First, Section 7.1 highlights the findings and contributions of the work, and maps them into the objectives that were set in Chapter 1. Next, few limitations of the work are listed in Section 7.2, followed by a discussion on some issues and concerns related to the proposed framework, which have been raised by reviewers and co-researchers, and the author's rebuttal in favor of the proposal. Finally, Section 7.4 concludes the chapter with a few suggestions for future work to further improve the proposed solution in the thesis.

7.1 Summary of Contributions in Relation to Research Objectives

In short, this research provided an alternative approach for nationwide health information exchange independent of other ongoing governmental approaches. The proposed approach was laid down in the form of a multi-component, distributed and a novel framework. At the core of this framework is an mPHR app that is owned by the patients and installed on their smartphones to carry their health information wherever they go. This app can exchange medical records with various legitimate HISs (run by healthcare providers) regardless of the deployed platform or database management system. The key to enable this exchange is the idea of a terminal device running another application that translates between the mPHR and the HIS at every site.

Those basic components and how they integrate do achieve the required level of interoperability. Modern wireless technologies built into smartphones provides the required connectivity. Depending on NFC technology for medical record transmission provided for the required level of security by eliminating certain types of attack such as eavesdropping and man-in-the-middle, due to the very short range of NFC transmission.

This in turn, eliminated the need to encrypt the data during the transfer. In addition, the framework is scalable and can accommodate indefinitely large number of users because of its distributed model; no central repository or processing server is involved. In the light of the defined objectives, the following points elaborate on the detailed list of contributions.

a) *Objective 1. To identify the current situation of nationwide health information exchange in Malaysia, and the requirements for solutions to implement secure and seamless exchange of health data between healthcare providers.*

   The status quo of health information exchange among healthcare providers in Malaysia has been clearly identified and outlined in the literature review. The Malaysian ministry of health has initiated the MyHIX project in order to enable hospitals to exchange patient health records. However, this project is still under development for the last few years and it continuously faces several challenges leading to significant delays. Interoperability and connectivity have been identified as the most important features to be achieved for exchanging health records. Besides these, other essential features such as security, standardization, scalability and availability must be taken under consideration.

b) *Objective 2. To propose a novel framework for nationwide HIE utilizing mPHRs and custom terminals at HIS points. The proposal should outline the overall architecture of the framework as well as the detailed design of individual components and their operation*.

   In Chapter 4, the targeted framework was proposed and its design was detailed. The proposed framework is a novel, practical, cost-efficient and readily deployable solution, innovatively using available technologies and requiring no changes to current infrastructure or functional systems. Three main components are key to the design of the framework: an mPHR at the side of the patient, the

legacy health information systems at the side of healthcare providers, and an interfacing device between the two, which is known as the terminal device.

c) *To implement a prototype version of the proposed framework with the help of the current tools and technologies in order to prove the concept of the solution*.

   A prototypic implementation of the three main components of the proposed framework was performed to demonstrate its feasibility and functions as well as illustrate one possible implementation. As described in Chapter 5, deployment of the proposed framework causes no changes to existing systems or infrastructure, and its implementation is possible using available commodity hardware and software technologies. One important and recurrent strategy followed is to adopt open source technologies whenever possible, which further reduces the costs of implementing the proposed framework.

d) *To validate the prototype version of the proposed framework based on a set of test cases generated from a simulated case study*.

   In Chapter 6, testing was done to the implemented prototypic version of the framework in order to provide a validation of the proposed solution. The individual components within the framework were tested based on a simulated case-study scenario, where a set of test cases had been generated to facilitate the testing process. The validation scenario covered major operational use cases and demonstrated that all the individual components within the framework were working properly according to the requirements and expectations.

In summary, all objectives have been achieved within the defined scope. However, limitations and opportunities for improvements do exist, which are discussed next.

7.2 Research Limitations

New solutions have their own drawbacks and limitations at the time of their introduction, and the proposed framework in this research is no exception. This section lists few limitations of the framework, while the next section discusses few issues and concerns that have been received from relevant experts and professionals in the field of healthcare informatics.

(a) Reliance on smartphones with NFC technology

As per the description in the previous chapters, the proposed framework depends on NFC to transfer the personal health records from the patient's mPHR to the terminal device of the healthcare provider and vice versa. Currently, not all smartphones are equipped with an NFC antenna, although the situation is changing and NFC is becoming a standard wireless interface like Bluetooth and Wi-Fi.

(b) Physical presence of the patient

The patient is required to be physically present in the location of healthcare provider each time an update for his or her health records is available or needed. In some cases, especially when conducting lab tests, the results may not be ready at the time of patient discharge; hence an extra visit to the healthcare provider is required in order to collect the lab results. However, this constraint is not introduced by the proposed framework specifically. Patient presence is always required in the current practice, other than the settings of telemedicine. The proposed framework just leverages the possession of smartphones by patients to implement health information exchange. One way to address this limitation is by allowing some data to be integrated into the mPHR client database from email attachments, and not only through NFC contacts.

*(c) **iOS operating system support***

Every aspect of developing the mPHR client is applicable to Apple devices (iPhone and iPad), except one major feature. Unfortunately, Apple did not add NFC hardware to its iOS-enabled devices until iPhone 6. Even then, NFC is only used with Apple Pay. In iPhone 7, the situation is slightly better, but still not enough to allow for the use case of reading and writing NFC messages freely between apps. It is believed, however, that it is a matter of time before Apple catches up with other manufacturers in supporting NFC, and then nothing prevents the same development in the context of the proposed framework to extend to iOS.

7.3 Discussion on Recurrent Issues and Concerns

One of the main challenges for HIE initiatives is the lack of stakeholder buy-in; in the first place, providers would like a compelling business case for participation in HIE. In addition, once a solution is accepted, financial sustainability emerges as a major concern to ensure longitudinal support for the solution. These issues have a similar impact on the adoption and the sustainability of the proposed approach by providers and consumers. However, the following lines argues that the nature of the proposed framework lends itself to an appealing solution that can address issues faced by other approaches for several reasons.

- Perceiving the HIE as a burden to providers affects their willingness to participate. In the context of the proposed framework, however, patients are doing the exchange, not the providers. In essence, the approach of the framework is shifting the problem of the providers from one of how to involve in HIE and manage the exchange process and its requirements and consequences into a (easier) problem of how to interface with patients in a new way. This is not the first time providers would have faced this kind of problem; the previous

movement into EHRs brought along new ways of interfacing with patients' data from manual recording into computerized data entry. Now, the move into HIE entails extending the method of interfacing into an automated process of device-based exchange.

- The adoption of the proposed solution requires only a minimal investment in developing a terminal app that is written only once and can be used for a long time with no or only a slight change. Admittedly, this point serves to lower the barrier to participation rather than attracting demand by incentives, but it can still be a good selling point compared with other solutions.
- The use of terminals can actually minimize the costs of the provider for patient administration management, even outside the frame of HIE; this prospect is evident when considering the required labor and processing time for manual data entry and update during a patient encounter.
- Another challenge facing other approaches of HIE is their integration into the provider workflow, where the exchanged data through channels of HIE are not easily incorporated into existing patient records. Interestingly, this is not an issue in the case of the proposed framework in this thesis, because the exchanged information is directly integrated into the local database more efficiently than would be achieved by any other manual or electronic mechanisms.

In the ideal case, the government would endorse the development of the mPHR client, probably by outsourcing to a professional organization, and then push toward adopting the whole solution by the providers, either directly or indirectly. One possible approach to influence the providers' support indirectly is by encouraging consumers to use the mPHR app and to prefer those providers who support its use. This process would be easy for patients if they have the option to select. In anyway, the consumers can be encouraged to ask for their data through the mPHR app whenever they visit a

provider. Eventually, public acceptance can drive the providers to adopt the solution out of business interest. Such public acceptance can be fueled by focused and organized publicity.

If users, nowadays, were offered a useful service, especially one that is endorsed by authorities and is free of charge, then they would probably avail of this service by the current norms. Unlike the case in other HIE approaches; users are not required to pay for the exchange function in the proposed framework. Users can even be provided with nominal incentives by enabling them to share selected segments of their data voluntarily for the purpose of anonymized reports with permission for reuse.

This framework can be adopted and utilized by interested parties as long as no effective mechanism exists to exchange data between healthcare centers. If the idea were accepted by a sufficient number of care providers or had the desired support of government health agencies, then several revenue streams would probably be formed from the following sources:

- The mPHR apps that run on patients' smartphones.
- Implementing the converter/translator apps on terminal devices for individual healthcare providers, perhaps on a contract basis. This service could be delegated to third-party developers because the specification of the standard format will be public, and the specific format of the database of the healthcare provider will be given by the provider itself.
- Providers of the proposed solution can also sell tablets (as terminal devices) pre-equipped with the translating apps for individual healthcare providers.

7.4 Future Work

This chapter is concluded with a few suggestions to improve the proposed solution in the future. First, the limitations of the work discussed previously is one viable place to start, especially the one related to the addition of an email option to send selected information. Second, the proper validation and evaluation of the framework is crucial for its acceptance in production. Future work should complete the development of a fully functional version of the mPHR app at the patient side, and add more data mapping fields between the selected HISs and the mPHR app.

The next step would be to pilot the system in certain healthcare centers and adding more hospitals to test the scalability of the framework. To enhance the adoption of the framework, it is possible to contact healthcare providers and offer to develop custom terminal apps for their legacy HIS as a step to connect with their patients who are using the client mPHR app.

REFERENCES

AeHIN. (2016). *The Hexagon - April to June 2016 issue*. https://aehin.hingx.org/Hexagon_AprilJune2016: Asia eHealth Information Network

Allaudin, F. S. (2013). *AeHIN General Meeting 2013: eHealth Updates in Malaysia*. https://aehin.hingx.org/1819; http://www.aehin.org/Sponsorships/COBIT/FazilahbintiShaikAllaudin.aspx: Asia eHealth Information Network.

Alliance, W.-F. (2016). "Wi-Fi Direct | Wi-Fi Alliance". *Available: http://www.wi-fi.org/discover-wi-fi/wi-fi-direct., Accessed On 12/1/2016.*

Ant Ozok, A., Wu, H., Garrido, M., Pronovost, P. J., & Gurses, A. P. (2014). Usability and perceived usefulness of personal health records for preventive health care: A case study focusing on patients' and primary care providers' perspectives. *Applied Ergonomics, 45*(3), 613-628. doi:http://dx.doi.org/10.1016/j.apergo.2013.09.005

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

Arm, J., Misik, S., Bradac, Z., & Kaczmarczyk, V. (2015). Android OS parameters measurement on S3C6410. *IFAC-PapersOnLine, 48*(4), 141-146. doi:http://dx.doi.org/10.1016/j.ifacol.2015.07.022

Bailey, J. E., Pope, R. A., Elliott, E. C., Wan, J. Y., Waters, T. M., & Frisse, M. E. (2013). Health Information Exchange Reduces Repeated Diagnostic Imaging for Back Pain. *Annals of emergency medicine, 62*(1), 16-24. doi:http://dx.doi.org/10.1016/j.annemergmed.2013.01.006

Barbarito, F., Pinciroli, F., Mason, J., Marceglia, S., Mazzola, L., & Bonacina, S. (2012). Implementing standards for the interoperability among healthcare providers in the public regionalized Healthcare Information System of the Lombardy Region. *Journal of Biomedical Informatics, 45*(4), 736-745. doi:http://dx.doi.org/10.1016/j.jbi.2012.01.006

Batistatos, M. C., Tsoulos, G. V., & Athanasiadou, G. E. (2012). Mobile telemedicine for moving vehicle scenarios: Wireless technology options and challenges. *Journal of Network and Computer Applications, 35*(3), 1140-1150. doi:http://dx.doi.org/10.1016/j.jnca.2012.01.003

Benli, S., Yaylacicegi, U., Vetter, R., Reinicke, B., & Mitchell, S. (2012). Information Security Blueprint for National Health Information Network. *Annals of the Master of Science in Computer Science and Information Systems at UNC Wilmington, 6*(1).

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2010). Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10

Rounds. In H. Gilbert (Ed.), *Advances in Cryptology – EUROCRYPT 2010* (Vol. 6110, pp. 299-319): Springer Berlin Heidelberg.

Blazona, B., & Koncar, M. (2007). HL7 and DICOM based integration of radiology departments with healthcare enterprise information systems. *International Journal of Medical Informatics, 76, Supplement 3*, S425-S432. doi:http://dx.doi.org/10.1016/j.ijmedinf.2007.05.001

Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS, 46*(2), 203-213.

Boneh, D., Joux, A., & Nguyen, P. (2000). Why Textbook ElGamal and RSA Encryption Are Insecure. In T. Okamoto (Ed.), *Advances in Cryptology — ASIACRYPT 2000* (Vol. 1976, pp. 30-43): Springer Berlin Heidelberg.

Brailer, D. J. (2005). Interoperability: the key to the future health care system. *HEALTH AFFAIRS-MILLWOOD VA THEN BETHESDA MA-, 24*, W5.

Burrows, J. H. (1995). *Secure hash standard*. Retrieved from

Burton, L. C., Anderson, G. F., & Kues, I. W. (2004). Using Electronic Health Records to Help Coordinate Care. *Milbank Quarterly, 82*(3), 457-481. doi:10.1111/j.0887-378X.2004.00318.x

Byrne, C. M., Mercincavage, L. M., Bouhaddou, O., Bennett, J. R., Pan, E. C., Botts, N. E., . . . Cromwell, T. (2014). The Department of Veterans Affairs' (VA) implementation of the Virtual Lifetime Electronic Record (VLER): Findings and lessons learned from Health Information Exchange at 12 sites. *International Journal of Medical Informatics, 83*(8), 537-547. doi:http://dx.doi.org/10.1016/j.ijmedinf.2014.04.005

Chen, C.-L., Yang, T.-T., & Shih, T.-F. (2014). A Secure Medical Data Exchange Protocol Based on Cloud Environment. *Journal of medical systems, 38*(9), 1-12. doi:10.1007/s10916-014-0112-3

Chhanabhai, P., & Holt, A. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine, 9*(1), 8.

Chou, D. (2011). Health Information Systems: Architectures and Strategies. *Jama, 306*(12), 1383-1384.

Cios, K. J., & William Moore, G. (2002). Uniqueness of medical data mining. *Artificial Intelligence in Medicine, 26*(1–2), 1-24. doi:http://dx.doi.org/10.1016/S0933-3657(02)00049-0

Coiera, E. (2009). Building a National Health IT System from the Middle Out. *Journal of the American Medical Informatics Association, 16*(3), 271-273. doi:10.1197/jamia.M3183

Coskun, V., Ozdenizci, B., & Ok, K. (2015). The Survey on Near Field Communication. *Sensors, 15*(6), 13348-13405.

Cruz Zapata, B., Hernández Niñirola, A., Idri, A., Fernández-Alemán, J., & Toval, A. (2014). Mobile PHRs Compliance with Android and iOS Usability Guidelines. *Journal of medical systems, 38*(8), 1-16. doi:10.1007/s10916-014-0081-6

Curran, K., Millar, A., & Mc Garvey, C. (2012). Near field communication. *International Journal of Electrical and Computer Engineering, 2*(3), 371.

Cushman, R., Froomkin, A. M., Cava, A., Abril, P., & Goodman, K. W. (2010). Ethical, legal and social issues for personal health records and applications. *Journal of Biomedical Informatics, 43*(5, Supplement), S51-S55. doi:http://dx.doi.org/10.1016/j.jbi.2010.05.003

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*: Springer Science & Business Media.

Developers, A. (2016). Near Field Communication. *https://developer.android.com/guide/topics/connectivity/nfc/index.html*.

Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE, 76*(5), 560-577. doi:10.1109/5.4442

Dixon, B. E., Vreeman, D. J., & Grannis, S. J. (2014). The long road to semantic interoperability in support of public health: Experiences from two states. *Journal of Biomedical Informatics, 49*(0), 3-8. doi:http://dx.doi.org/10.1016/j.jbi.2014.03.011

Dixon, B. E., Zafar, A., & Overhage, J. M. (2010). A Framework for evaluating the costs, effort, and value of nationwide health information exchange. *Journal of the American Medical Informatics Association, 17*(3), 295-301. doi:10.1136/jamia.2009.000570

Donahue, M. (2009). OpenEMR and its community. *Entry in GPL Medicine Wiki, accessed, 4*.

Eden, K. B., Totten, A. M., Kassakian, S. Z., Gorman, P. N., McDonagh, M. S., Devine, B., . . . Hersh, W. R. (2016). Barriers and facilitators to exchanging health information: a systematic review. *International Journal of Medical Informatics, 88*, 44-51. doi:https://doi.org/10.1016/j.ijmedinf.2016.01.004

Elenkov, N. (2012). Using Password-based Encryption on Android. *https://nelenkov.blogspot.my/2012/04/using-password-based-encryption-on.html?view=flipcard*.

Elsevier. (2015). Healthcare organisations struggle to maintain security. *Network Security, 2015*(10), 1-2. doi:http://dx.doi.org/10.1016/S1353-4858(15)30084-2

Evans, J. A. (1999). Electronic medical records system: Google Patents.

Flores, A. (2010). Secure exchange of information in electronic health records.

Fontaine, P., Ross, S. E., Zink, T., & Schilling, L. M. (2010). Systematic Review of Health Information Exchange in Primary Care Practices. *The Journal of the*

American Board of Family Medicine, 23(5), 655-670. doi:10.3122/jabfm.2010.05.090192

Forum, N. (2016). Home - NFC Forum | NFC Forum. *Available: http://nfc-forum.org/*.

FreeMED. (2017). FreeMED Software Foundation. *FreeMED Software Foundation," 2017. [Online]*.

Frisse, M. E., Johnson, K. B., Nian, H., Davison, C. L., Gadd, C. S., Unertl, K. M., . . . Chen, Q. (2011). The financial impact of health information exchange on emergency department care. *Journal of the American Medical Informatics Association*. doi:10.1136/amiajnl-2011-000394

Garets, D., & Davis, M. (2006). Electronic medical records vs. electronic health records: yes, there is a difference. *Policy white paper. Chicago, HIMSS Analytics*.

Genitsaridi, I., Kondylakis, H., Koumakis, L., Marias, K., & Tsiknakis, M. (2015). Evaluation of personal health record systems through the lenses of EC research projects. *Computers in Biology and Medicine*(0). doi:http://dx.doi.org/10.1016/j.compbiomed.2013.11.004

Ghani, M. A. (2008). *An Integrated and Distributed Framework for a Malaysian Telemedicine System (MYtel)*: Coventry University.

Gibson, R. F. (2017). Health Information Exchange, Brian E. Dixon. Elsevier/Academic Press, Cambridge, MA (2016). 361 pp., ISBN: 978-0-12-803135-3. *Journal of Biomedical Informatics, 67*, 49-50. doi:https://doi.org/10.1016/j.jbi.2017.02.002

Gonzalez, T. (2007). A Reflection Attack on Blowfish. *Journal of Latex Files, 6*(1).

Gritzalis, D., & Lambrinoudakis, C. (2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics, 73*(3), 305-309. doi:http://dx.doi.org/10.1016/j.ijmedinf.2003.12.011

Gupta, V., Gupta, S., Chang, S., & Stebila, D. (2002). *Performance analysis of elliptic curve cryptography for SSL*. Paper presented at the Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA.

HAPI. (2016). The Open Source HL7 API for Java. *http://hl7api.sourceforge.net/index.html*.

Hargreaves, J. S. (2010). Will electronic personal health records benefit providers and patients in rural America? *Telemedicine and e-Health, 16*(2), 167-176.

Harvey, M. J., & Harvey, M. G. (2014). Privacy and security issues for mobile health platforms. *Journal of the Association for Information Science and Technology, 65*(7), 1305-1318.

He, Y., & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International*

Journal of Medical Informatics, 84(11), 941-949. doi:http://dx.doi.org/10.1016/j.ijmedinf.2015.08.010

Hermans, J., Vercauteren, F., & Preneel, B. (2010). Speed Records for NTRU. In J. Pieprzyk (Ed.), *Topics in Cryptology - CT-RSA 2010* (Vol. 5985, pp. 73-88): Springer Berlin Heidelberg.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs, 24*(5), 1103-1117.

Hisan, D. A. (2012). *Malaysian Health Information Exchange (MyHIX)*. http://ngis.mygeoportal.gov.my/.

HL7. (2017a). Introduction to HL7 Standards *Health Level Seven International*. http://www.hl7.org/implement/standards/.

HL7. (2017b). *PHR-S FM Personal Health Record System Functional Model (PHR-S FM)*. https://www.hl7.org/implement/standards/product_brief.cfm?product_id=88.

Hoffstein, J., Pipher, J., & Silverman, J. (1998). NTRU: A ring-based public key cryptosystem. In J. Buhler (Ed.), *Algorithmic Number Theory* (Vol. 1423, pp. 267-288): Springer Berlin Heidelberg.

Househ, M. S., Borycki, E. M., Rohrer, W. M., & Kushniruk, A. W. (2014). Developing a framework for meaningful use of personal health records (PHRs). *Health Policy and Technology, 3*(4), 272-280. doi:http://dx.doi.org/10.1016/j.hlpt.2014.08.009

Huang, K.-H., Hsieh, S.-H., Chang, Y.-J., Lai, F., Hsieh, S.-L., & Lee, H.-H. (2010). Application of Portable CDA for Secure Clinical-document Exchange. *Journal of medical systems, 34*(4), 531-539. doi:10.1007/s10916-009-9266-9

IDC. (2016). IDC: Smartphone OS Market Share 2016, 2015. *http://www.idc.com/prodserv/smartphone-os-market-share.jsp*.

Iezzoni, L. I. (1997). Assessing Quality Using Administrative Data. *Annals of Internal Medicine, 127*(8_Part_2), 666-674. doi:10.7326/0003-4819-127-8_Part_2-199710151-00048

Jurišic, A., & Menezes, A. (1997). Elliptic curves and cryptography. *Dr. Dobb's Journal*, 26-36.

Kaelber, D. C., & Bates, D. W. (2007). Health information exchange and patient safety. *Journal of Biomedical Informatics, 40*(6, Supplement), S40-S45. doi:http://dx.doi.org/10.1016/j.jbi.2007.08.011

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. doi:10.1197/jamia.M2547

Kaliski, B. (2000). PKCS# 5: Password-based cryptography specification version 2.0.

Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. *ACM Ubiquity, 9*(20), 20-26.

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

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: An evaluation of features and functionality. *International Journal of Medical Informatics, 81*(9), 579-593. doi:http://dx.doi.org/10.1016/j.ijmedinf.2012.04.007

Khoumbati, K., Themistocleous, M., & Irani, Z. (2005, 03-06 Jan. 2005). *Integration Technology Adoption in Healthcare Organisations: A Case for Enterprise Application Integration.* Paper presented at the System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on.

Kiah, M. L. M., Haiqi, A., Zaidan, B. B., & Zaidan, A. A. (2014). Open source EMR software: Profiling, insights and hands-on analysis. *Computer Methods and Programs in Biomedicine, 117*(2), 360-382. doi:http://dx.doi.org/10.1016/j.cmpb.2014.07.002

Kobayashi, S. (2012). Open source software development on medical domain *Modern Information Systems*: Intech.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation, 48*(177), 203-209.

Kocher, P. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In N. Koblitz (Ed.), *Advances in Cryptology — CRYPTO '96* (Vol. 1109, pp. 104-113): Springer Berlin Heidelberg.

Kripalani, S., LeFevre, F., Phillips, C. O., Williams, M. V., Basaviah, P., & Baker, D. W. (2007). Deficits in communication and information transfer between hospital-based and primary care physicians: implications for patient safety and continuity of care. *Jama, 297*(8), 831-841.

Kuperman, G. J. (2011). Health-information exchange: why are we doing it, and what are we doing? *Journal of the American Medical Informatics Association, 18*(5), 678-682. doi:10.1136/amiajnl-2010-000021

Kuperman, G. J., Blair, J. S., Franck, R. A., Devaraj, S., Low, A. F. H., & Group, f. t. N. T. I. C. S. C. W. (2010). Developing data content specifications for the Nationwide Health Information Network Trial Implementations. *Journal of the American Medical Informatics Association, 17*(1), 6-12. doi:10.1197/jamia.M3282

Lee, J. S., Su, Y. W., & Shen, C. C. (2007, 5-8 Nov. 2007). *A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi.* Paper presented at the

Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE.

Lee, M., Delaney, C., & Moorhead, S. (2007). Building a personal health record from a nursing perspective. *International Journal of Medical Informatics, 76, Supplement 2*(0), S308-S316. doi:http://dx.doi.org/10.1016/j.ijmedinf.2007.05.010

Lenert, L., Sundwall, D., & Lenert, M. E. (2012). Shifts in the architecture of the Nationwide Health Information Network. *Journal of the American Medical Informatics Association, 19*(4), 498-502. doi:10.1136/amiajnl-2011-000442

Li, J.-S., Zhang, X.-G., Chu, J., Suzuki, M., & Araki, K. (2012). Design and Development of EMR Supporting Medical Process Management. *Journal of medical systems, 36*(3), 1193-1203. doi:10.1007/s10916-010-9581-1

Liang, X., Vicente, J., Saez, C., Peet, A., Gibb, A., Lewis, P., . . . Dupplaw, D. (2008, 4-7 March 2008). *A Security Model and its Application to a Distributed Decision Support System for Healthcare.* Paper presented at the Availability, Reliability and Security, 2008. ARES 08. Third International Conference on.

Liu, J., Huang, X., & Liu, J. K. (2014). Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. *Future Generation Computer Systems*(0). doi:http://dx.doi.org/10.1016/j.future.2014.10.014

Liu, W., Park, E., & Krieger, U. (2012). *eHealth interconnection infrastructure challenges and solutions overview.* Paper presented at the e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on.

Luo, J. N., Yang, M. H., & Huang, S.-Y. (2016). An Unlinkable Anonymous Payment Scheme based on near field communication. *Computers & Electrical Engineering, 49*, 198-206. doi:http://dx.doi.org/10.1016/j.compeleceng.2015.08.007

Lupse, O. S., Vida, M. M., & Stoicu-Tivadar, L. (2012). *Cloud computing and interoperability in healthcare information systems.* Paper presented at the INTELLI 2012, The First International Conference on Intelligent Systems and Applications.

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

Mat Som, M. H., Norali, A. N., & Ali, M. S. A. (2010, 3-5 Oct. 2010). *Telehealth in Malaysia — An overview.* Paper presented at the Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on.

McHome, S., Sachdeva, S., & Bhalla, S. (2010, 1-3 Aug. 2010). *A brief survey: Usability in healthcare.* Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On.

MIMOS. (2013). *MIMOS collaborates with Health Ministry to develop Healthcare IT*. http://www.mosti.gov.my/berita/mimos-collaborates-with-health-ministry-to-develop-healthcare-it/: www.mosti.gov.my.

Ming, L., Shucheng, Y., Yao, Z., Kui, R., & Wenjing, L. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *Parallel and Distributed Systems, IEEE Transactions on, 24*(1), 131-143. doi:10.1109/tpds.2012.97

Miranda, M., Salazar, M., Portela, F., Santos, M., Abelha, A., Neves, J., & Machado, J. (2012). Multi-agent Systems for HL7 Interoperability Services. *Procedia Technology, 5*(0), 725-733. doi:http://dx.doi.org/10.1016/j.protcy.2012.09.080

MOH. (1997). *Malaysia's Telemedicine Blueprint: Leading Healthcare into the Information Age*. http://www.moh.gov.my/images/gallery/Telemedicine/TelemedicineBlueprint.pdf: www.moh.gov.my.

Mon, D., Ritter, J., Spears, C., & Van Dyke, P. (2008). PHR system functional model. *HL7 PHR Standard*.

Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Systems, 64*, 108-124. doi:http://dx.doi.org/10.1016/j.future.2016.02.020

Morrison, Z., Robertson, A., Cresswell, K., Crowe, S., & Sheikh, A. (2011). Understanding Contrasting Approaches to Nationwide Implementations of Electronic Health Record Systems: England, the USA and Australia. *Journal of Healthcare Engineering, 2*(1). doi:10.1260/2040-2295.2.1.25

Mylonas, A., Dritsas, S., Tsoumas, B., & Gritzalis, D. (2011, 18-21 July 2011). *Smartphone security evaluation The malware attack case.* Paper presented at the Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on.

Northrop, L., Feiler, P., Gabriel, R. P., Goodenough, J., Linger, R., Longstaff, T., . . . Sullivan, K. (2006). {Ultra-Large-Scale Systems}-The Software Challenge of the Future.

OpenEMR. (2016). OpenEMR Project. *http://www.open-emr.org*.

Park, H., Lee, S.-i., Kim, Y., Heo, E.-Y., Lee, J., Park, J. H., & Ha, K. (2013). Patients' perceptions of a health information exchange: A pilot program in South Korea. *International Journal of Medical Informatics, 82*(2), 98-107. doi:http://dx.doi.org/10.1016/j.ijmedinf.2012.05.001

Passwords, S. (2011). HIPAA: privacy, security, and pharmacy information technology. *US Pharm, 36*(11), 79-81.

Payne, T. H., Detmer, D. E., Wyatt, J. C., & Buchan, I. E. (2011). National-scale clinical information exchange in the United Kingdom: lessons for the United

States. *Journal of the American Medical Informatics Association, 18*(1), 91-98. doi:10.1136/jamia.2010.005611

Perlner, R. A., & Cooper, D. A. (2009). *Quantum resistant public key cryptography: a survey*. Paper presented at the Proceedings of the 8th Symposium on Identity and Trust on the Internet, Gaithersburg, Maryland.

Rea, S., Pathak, J., Savova, G., Oniki, T. A., Westberg, L., Beebe, C. E., . . . Huff, S. M. (2012). Building a robust, scalable and standards-driven infrastructure for secondary use of EHR data: the SHARPn project. *Journal of Biomedical Informatics, 45*(4), 763-771.

Regidor, E. (2004). The use of personal data from medical records and biological materials: ethical perspectives and the basis for legal restrictions in health research. *Social Science & Medicine, 59*(9), 1975-1984. doi:http://dx.doi.org/10.1016/j.socscimed.2004.02.032

Rivest, R. (1995). The RC5 encryption algorithm. In B. Preneel (Ed.), *Fast Software Encryption* (Vol. 1008, pp. 86-96): Springer Berlin Heidelberg.

Rivest, R. L., Robshaw, M., Sidney, R., & Yin, Y. L. (1998). *The RC6TM block cipher.* Paper presented at the First Advanced Encryption Standard (AES) Conference.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM, 21*(2), 120-126. doi:10.1145/359340.359342

Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., & Detmer, D. E. (2007). Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association, 14*(1), 1-9. doi:http://dx.doi.org/10.1197/jamia.M2273

Salah, I. K., Darwish, A., & Oqeili, S. (2006). Mathematical Attacks on RSA Cryptosystem. *Journal of Computer science, 2*(8).

Schneier, B. (1994a). The Blowfish encryption algorithm. *Dr Dobb's Journal-Software Tools for the Professional Programmer, 19*(4), 38-43.

Schneier, B. (1994b). Description of a new variable-length key, 64-bit block cipher (Blowfish). In R. Anderson (Ed.), *Fast Software Encryption* (Vol. 809, pp. 191-204): Springer Berlin Heidelberg.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). Performance comparison of the AES submissions.

Shapiro, J. S., Kannry, J., Lipton, M., Goldberg, E., Conocenti, P., Stuard, S., . . . Kuperman, G. (2006). Approaches to Patient Health Information Exchange and Their Impact on Emergency Medicine. *Annals of emergency medicine, 48*(4), 426-432. doi:http://dx.doi.org/10.1016/j.annemergmed.2006.03.032

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

Silverman, D. P. (2001). Data network security system and method: Google Patents.

Som, M. M., Norali, A., & Ali, M. M. (2010). *Telehealth in Malaysia—An overview.* Paper presented at the Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on.

Song, M., Liu, K., Abromitis, R., & Schleyer, T. L. (2013). Reusing electronic patient data for dental clinical research: A review of current status. *Journal of Dentistry, 41*(12), 1148-1163. doi:http://dx.doi.org/10.1016/j.jdent.2013.04.006

Song, Y.-T., Pak, J., Kalabins, A., & Fouché, S. (2017). *Standard-based patient-centered personal health record system.* Paper presented at the Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication.

Sprivulis, P., Walker, J., Johnston, D., Pan, E., Adler-Milstein, J., Middleton, B., & Bates, D. W. (2007). The economic benefits of health information exchange interoperability for Australia. *Australian Health Review, 31*(4), 531-539. doi:http://dx.doi.org/10.1071/AH070531

Standard, N.-F. (2001). Announcing the Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication, 197*.

Sucurovic, S. (2007). Implementing security in a distributed web-based EHCR. *International Journal of Medical Informatics, 76*(5–6), 491-496. doi:http://dx.doi.org/10.1016/j.ijmedinf.2006.09.017

Sun, H., Depraetere, K., De Roo, J., Mels, G., De Vloed, B., Twagirumukiza, M., & Colaert, D. (2015). Semantic processing of EHR data for clinical research. *Journal of Biomedical Informatics, 58*, 247-259.

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.

Tansel, A. U. (2013). Innovation through Patient Health Records. *Procedia - Social and Behavioral Sciences, 75*(0), 183-188. doi:http://dx.doi.org/10.1016/j.sbspro.2013.04.021

Tom, J. O., Chen, C., & Zhou, Y. Y. (2014). Personal Health Record Use and Association with Immunizations and Well-Child Care Visits Recommendations. *The Journal of Pediatrics, 164*(1), 112-117. doi:http://dx.doi.org/10.1016/j.jpeds.2013.08.046

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues.

International Journal of Medical Informatics, 78(3), 141-160. doi:10.1016/j.ijmedinf.2008.06.013

Van Gorp, P., Comuzzi, M., Jahnen, A., Kaymak, U., & Middleton, B. (2014). An open platform for personal health record apps with platform-level privacy protection. *Computers in Biology and Medicine, 51*(0), 14-23. doi:http://dx.doi.org/10.1016/j.compbiomed.2014.04.019

Vest, J. R. (2012). Health information exchange: national and international approaches. *Advances in health care management, 12*, 3-24.

Vest, J. R., & Gamm, L. D. (2010). Health information exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association, 17*(3), 288-294. doi:10.1136/jamia.2010.003673

ViaMED. (2017). Retrieved from https://sites.google.com/a/viamed.com.my/viamed/

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *HEALTH AFFAIRS-MILLWOOD VA THEN BETHESDA MA-, 24*, W5.

Wang, X., Yin, Y., & Yu, H. (2005). Finding Collisions in the Full SHA-1. In V. Shoup (Ed.), *Advances in Cryptology – CRYPTO 2005* (Vol. 3621, pp. 17-36): Springer Berlin Heidelberg.

Wang, X., & Yu, H. (2005). *How to break MD5 and other hash functions.* Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer, 45*(12), 0052-0058.

Want, R. (2011). Near field communication. *IEEE Pervasive Computing, 3*(10), 4-7.

Wasserman, R. C. (2011). Electronic Medical Records (EMRs), Epidemiology, and Epistemology: Reflections on EMRs and Future Pediatric Clinical Research. *Academic Pediatrics, 11*(4), 280-287. doi:http://dx.doi.org/10.1016/j.acap.2011.02.007

Yeager, V., Walker, D., Cole, E., Mora, A., & Diana, M. (2014). Factors Related to Health Information Exchange Participation and Use. *Journal of medical systems, 38*(8), 1-9. doi:10.1007/s10916-014-0078-1

LIST OF PUBLICATIONS AND PAPERS PRESENTED

Mohamed Abdulnabi, Ahmed Al-Haiqi, M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan, Muzammil Hussain. (2017). A Distributed Framework for Health Information Exchange Using Smartphone Technologies. Journal of Biomedical Informatics, 69, 230-250. [Q1-ISI] (ISI-Indexed).

B.B. Zaidan, Ahmed Haiqi, A.A. Zaidan, Mohamed Abdulnabi, M. L. Mat Kiah & Hussaen Muzamel. 2015. A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy. Journal of Medical Systems 39:51. [Q2-ISI] (ISI-Indexed).

A.A. Zaidan, B.B. Zaidan, Muzammil Hussain, Ahmed Haiqi, M.L. Mat Kiah & Mohamed Abdulnabi. 2015. Multi- Criteria Analysis for OS-EMR Software Selection Problem: A Comparative Study. Decision Support Systems 78:15-27. [Q1-ISI] (ISI-Indexed).

M.L Mat Kiah, Mohamed S.Nabi, B.B Zaidan & A.A Zaidan. 2013. An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP-XML and SHA-1. Journal of Medical Systems 37:9971. [Q2-ISI] (ISI-Indexed).

M.L.M. Kiah, B.B Zaidan, A.A.Zaidan, Mohamed Nabi & Rabiu Ibraheem. 2014. MIRASS: Medical Informatics Research Activity Support System using Information Mashup Network. Journal of Medical Systems 38 (37):1-15. [Q2-ISI] (ISI-Indexed).

Nabi, M. S., Mat Kiah, M. L., Zaidan, A. A., & Zaidan, B. B. 2013. Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records. In Future Generation Communication Technology (FGCT), 2013 Second International IEEE Conference. 93- 97. (ISI-Indexed).