PRIVACY AND SECURITY OF STORING PATIENTS' DATA IN THE CLOUD

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Institute for Sustainable Industries and Liveable Cities (ISILC)

Victoria University

by

Pasupathy Vimalachandran

September 2019

ABSTRACT

PRIVACY AND SECURITY OF STORING PATIENTS' DATA IN THE CLOUD

Pasupathy Vimalachandran, Ph.D.

Victoria University 2019

A better health care service must ensure patients receive the right care, in the right place, at the right time. In enabling better health care, the impact of technology is immense. Technological breakthroughs are revolutionising the way health care is being delivered. To deliver better health care, sharing health information amongst health care providers who are involved with the care is critical. An Electronic Health Record (EHR) platform is used to share the health information among those health care providers faster, as a result of technological advancement including the Internet and the Cloud.

However, when integrating such technologies to support the provision of health care, they lead to major concerns over privacy and security of health sensitive information. The privacy and security concerns include a wide range of ethical and legal issues associated with the system. These concerns need to be considered and addressed for the implementation of EHR systems. In a shared environment like EHRs, these concerns become more significant. In this thesis, the author explores and discusses the situations where these concerns do arise in a health care environment. This thesis also covers different attacks that have targeted health care information in the past, with potential solutions for every attack identified. From these findings, the proposed system is designed and developed to provide considerable security assurance for a health care organisation when using the EHR systems. Furthermore, the My Health Record (MyHR) system is introduced in Australia to allow an individual's doctors and other health care providers to access the individual's health information. Privacy and security in using MyHR is a major challenge that impacts its usage.

Taking all these concerns into account, the author will also focus on discussing and analysing major existing access control methods, various threats for data privacy and security concerns over EHR use and the importance of data integrity while using MyHR or any other EHR systems. To preserve data privacy and security and prevent unauthorised access to the system, the author proposes a three-tier security model. In this three-tier security model, the first tier covers an access control mechanism, an Intermediate State of Databases (ISD) is included in the second tier and the third layer involves

cryptography/data encryption and decryption. These three tiers, collectively, cover different forms of attacks from different sources including unauthorised access from inside a health care organisation. In every tier, a specific technique has been utilised. In tier one, an Improved Access Control Mechanism (IACM) known as *log-in pair*, *pseudonymisation* technique is proposed in tier two and a special new encryption and decryption algorithm has been developed and used for tier three in the proposed system.

In addition, the design, development, and implementation of the proposed model have been described to enable and evaluate the operational protocol.

Problem 1. Non-clinical staff including reception, admin staff access sensitive health clinical information (insiders).

Solution 1. An improved access control mechanism named *log-in pair* is introduced and occupied in tier one.

Problem 2. Researchers and research institutes access health data sets for research activities (outsiders).

Solution 2. *Pseudonymisation* technique, in tier two, provides de-identified required data with relationships, not the sensitive data.

Problem 3. The massive amount of sensitive health data stored with the EHR system in the Cloud becomes more vulnerable to data attacks.

Solution 3. A new encryption and decryption algorithm is achieved and used in tier three to provide high security while storing the data in the Cloud.

DOCTOR OF PHILOSOPHY DECLARATION

I, Pasupathy Vimalachandran, declare that the PhD thesis entitled *Privacy and Security of Storing Patients' Data in the Cloud* is no more than 100,000 words in length including quotes and exclusive of tables, figures, appendices, bibliography, references and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work.

Signature:  Date: 11 /09/ 2019

ACKNOWLEDGEMENTS

My sincere gratitude goes to everyone who supported me through this long journey.

First and foremost, I am indebted to my principal supervisor, Professor Hua Wang, for providing assistance and guidance to me throughout the course of my doctoral program at Victoria University. I also would like to thank my associate supervisor, Professor Yanchun Zhang for his support and encouragement.

I would like to thank all my family members and relatives who have given me moral support throughout this program.

PUBLICATIONS

Refereed conference papers:

Pasupathy Vimalachandran, Yanchun Zhang, Jinli Cao, Lili Sun, Jianming Yong: Preserving Data Privacy and Security in Australian My Health Record System: A Quality Health Care Implication. Preserving Data Privacy and Security in Australian My Health Record System: A Quality Health Care Implication: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part II. WISE (2) 2018: 111-120.

Pasupathy Vimalachandran, Hua Wang, Yanchun Zhang, Ben Heyward, Yueai Zhao: Preserving Patient-centred Controls in Electronic Health Record Systems: A Reliance-based Model Implication. International Conference on Orange Technologies (ICOT) 2017. Melbourne, Australia.

Pasupathy Vimalachandran, Hua Wang, Yanchun Zhang, Guangping Zhuo, Hongbo Kuang. Cryptographic Access Control in Electronic Health Record Systems: A Security Implication. Web Information Systems Engineering – WISE 2017: 18th International Conference, Puschino, Russia, October 7-11, 2017, Proceedings, Part II. WISE (2) 2017: 540-549

Pasupathy Vimalachandran, Hua Wang, Yanchun Zhang, Ben Heyward, F. Whittaker: Ensuring Data Integrity in Electronic Health Records: A Quality Health Care Implication.2016 International Conference on Orange Technologies (ICOT).CoRR abs/1802.00577 (2018)

Pasupathy Vimalachandran, Hua Wang, Yanchun Zhang. Securing Electronic Medical Record and Electronic Health Record Systems Through an Improved Access Control. Health Information Science: 4th International Conference, HIS 2015, Melbourne, Australia, May 28-30, 2015, Proceedings. 17-30.

Refereed Journal articles:

Pasupathy Vimalachandran, Hua Wang, Yu Zhang, G. Zhuo. The Australian PCEHR System: Ensuring Privacy and Security through an Improved Access Control Mechanism. EAI Endorsed Trans. Scalable Information Systems 3(8): e4 (2016).

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ABAC	Attribute Based Access Control
ABE	Attribute Based Encryption
ACeH	Australian Commission for Electronic Health
ACM	Access Control Mechanism
ACP	Access Control Policy
ADR	Adverse Drug Events
AHS	Allied Health Services
AMA	Australian Medical Association
BIS	Business Intelligence System
BP	Best Practice
BPOS	Business Productivity Online Suite
BYOC	Bring Your Own Cloud
CCD	Continuity of Care Document
CCR	Continuity of Care Record
CDA	Clinical Document Architecture
CDN	Content Delivery Networks
CEM	Chief Executive of Medicare
CHI	Canadian Health Infoway
CISSP	Certified Information System Security Professional
CP-ABE	Cipher Text Attribute Based Encryption
CPGA	Canadian Provincial Government Agency
CRM	Customer Relationship Management
CS	Clinical System
CTAC	Clinical and Technical Advisory Committee
DAC	Discretionary Access Control
DBMS	Database Management System
DDoS	Distributed Denial of Service
DHS	Department of Human Services
DOH	Department of Health
DOM	Document-Oriented Methodology
DSD	Defence Signals Directorate

DSS	Decision Support System
EC2	Elastic Compute Cloud
eHealth	Electronic Health
EHR	Electronic Health Record
EMR	Electronic Medical Record
EV	Event Summary
GP	General Practitioners
GSM	Global System for Mobile Communication
HI	Healthcare Identifier
HIE	Health Information Exchange
HIS	Health Information System
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
HPOS	Health Professional Online Services
IaaS	Infrastructure as a Service
IACM	Improved Access Control Mechanism
IAI	Individual Account Identifier
IIN	Issuer Identifier Number
IP	Internet Protocol
IPS	Intrusion Prevention System
ISD	Intermediate State of Database
ISD	Intermediate State of Database
ISF	Information Security Forum
IT	Information Technology
JAC	Jurisdictional Advisory Committee
JHMI	Johns Hopkins Medical Institution
MAC	Mandatory Access Control
MBS	Medicare Benefits Scheme
MD	Medical Director
MHV	Microsoft Health Vault
MII	Major Industry Identifier
MML	Medical Markup Language

MyHR	My Health Record
NASH	National Authentication Service for Health
NDB	Notifiable Data Breaches
NEHTA	National Electronic Health Transition Authority
NEIF	National Electronic Health Interoperability Framework
NIST	National Institute of Standards and Technology
NLC	New London Consulting
NHS	National Health Services
OAIC	Office of the Australian Information Commissioner
OOM	Object-Oriented Methodology
ORLP	Oxford Record Linkage Project
PaaS	Platform as a Service
PBAC	Purpose-Based Access Control
PBS	Pharmaceutical Benefits Scheme
PCEHR	Personally Controlled Electronic Health Record
PDF	Portable Document Format
PEKS	Public Key Encryption with Keyword Search
PHI	Personal Health Information
PHR	Personal Health Records
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMS	Patient or Practice Management System or Software
PSC	Privacy and Security Committee
RACGP	Royal Australians College of General Practitioners
RBAC	Role-Based Access Control
RDA	Restricting Database Access
RU	Rutgers University
SaaS	Software as a Service
SAIF	Service Aware Interoperability Framework
SAS	Statement on Auditing Standards
SCoH	Standing Council on Health
SHA	Secure Hash Algorithm

SHS	Shared Health Summary
SLCM	Selection of Software Life Cycle Model
SMF	System Monitoring Facility
SO	System Operator
SQL	Structured Query Language / Structured Programming Language
SSCCR	Standard Specification for Community of Care Record
TAC	Table Access Control
USA	United States of America
WHO	World Health Organisation
WPF	World Privacy Forum
XML	eXtensible Markup Language

Introduction

Better health care is imperative to maintain and to improve someone's health. Accessing health care not only keeps people healthier and safer, but it is also the right of the citizens of a country. Health care is one of the few rapid growing sectors where modern technology is progressively being used and established to get the most appropriate and positive outcomes. Because of the application, the impact on modern technology in health care is enormous. A broad range of machines are used in health care through activities like diagnosis, prevention, and treatment. For example, Magnetic Resonance Imaging (MRI) is one of the major technological developments in health care, particularly in diagnosis. Additionally, to deliver high-quality health care to a patient, the right decision at the right time is vital. This decision making must occur based on the patient's past medical history and other linked health information including allergy or adverse reaction, current medication and immunisation. Therefore, important health information is needed at the point of care to maintain a high-quality health care service. To satisfy this prerequisite, using modern technologies, especially the Cloud computing concept, an Electronic Health Record (EHR) is introduced.

Furthermore, most of the time, more than one health care provider is involved in patient care. For instance, consider a diabetic patient's journey, general practitioner, practice nurse, pharmacist, diabetic educator, dietician, medical specialist, and more health care providers may be involved. Hence, the purpose of the EHR system is not only to ensure the availability of the system when it is needed, but it also must include the patient's up to date accurate health information from every health care provider that the patient has visited in the past.

While ensuring wider availability for all health care providers to keep the information up-to-date and accurate and then easy accessibility at the point of care, EHR systems challenge several privacy and security issues. These issues impact the wider adoption and usage of the system, a good example is the Australian My Health Record (MyHR). The MyHR is one of the many EHR systems that have been introduced to improve the quality and the

cost-efficiency of health care in Australia. There has been a lack of confidence in the uptake and usage of the MyHR system in Australia. Privacy and security settings of the MyHR reduce the uptake and eventually persuade consumers to conceal their sensitive health information. As a result, their treatment may be compromised. Hence, addressing those privacy and security issues and proposing an appropriate security model for the MyHR system is crucial to increase the usage of the system.

1.1 Background

EHRs have become a powerful tool in modern health care delivery. While EHR systems replace paper-based medical records electronically, they also facilitate faster access the health information to relevant health care providers. EHRs have greatly improved the safety and quality of health care delivery by increasing access to health information, reducing illegibility and enabling closer overseeing of clinical care processes.

1.1.1 Development of Electronic Medical Records and Electronic Health Records

In an Electronic Health (eHealth) world, the words Electronic Medical Records (EMR) and Electronic Health Record (EHR) are used very commonly. Most people think that both EMR and EHR mean the same, but that is not correct. Even those in the health professions who use the technology every day tend to confuse EMR and EHR, perhaps using the two terms interchangeably, but there is a difference [21]. EHRs are designed to follow a patient from one health care provider to another and one health care provider organisation to another, throughout their lives. In other words, the EHR system must be available beyond a health care provider organisation, with maybe state or national level or even international level. EHRs are also designed to provide a complete picture of a patient's health information including allergies, current medications, medical histories, and immunisations. An EMR, on the other hand, replaces the paper-based medical records for a single practice (primarily) for a practice level to show a clear picture of a patient's journey within the practice and the medication prescribed and progress notes of each visit by the patient. In other words, while EHRs can be shared among health care provider organisations, EMRs are designed to remain in a health care provider organisation.
In practical examples [22],

- An EMR records immunisation data, but an EHR enables electronic sharing of that information with the government, school, or workplace clinicians.

- A primary care practice can enter the report from a patient's diagnostic imaging study in an EMR, but the radiologist can upload digital images and notes into the patient's EHR.
- A patient can request that information from the EMR be transmitted to a consulting physician, but multiple authorised providers can view and add information to an EHR, enabling interactive communication and care coordination.

Both EMR and EHR will be discussed throughout this document. It is, therefore, important to understand the difference between them.

1.1.2 Electronic Medical Record

In the health care sector, the first attempts at creating digital versions of electronic medical records (EMR) were made in 1962, in the Oxford Record Linkage Project (ORLP) [137]. EMR is a computerised version of a paper-based medical record that provides a digital version of a patient's health-associated information created by an authorised health care provider, in most cases by the usual general practitioner of the patient. To create, gather, manage and record health information several computer software programs are used. They are also usually known as Practice or Patient Management System or Software (PMS) or Clinical Systems (CS). PMS is referred to as software that is regulated as a medical device. PMS is software that is also used to acquire medical information from a medical device to be used in the treatment or diagnosis of a patient [23].

A PMS is usually used by a health care provider organisation to improve their daily functions effectively, and to provide high-quality health care and its associated services for their consumers. Expanded Internet access and the advent of Cloud-based software systems have dramatically sustained the functionality and service range that practice management software systems can deliver [24]. It has also facilitated a significant reduction in product distribution and support costs which have resulted in the proliferation of a large number of service offerings [24]. Hence, to work with EHR, the PMS also assists with billing, claiming, reporting and workflow. Health care provider organisations are now considering opting for the Cloud computing PMS systems because it is more cost-effective and easier to maintain. By selecting a Cloud-based system that is simple and easy to operate, it can make an initial adoption and integration as smooth as possible compare to the server-client model. That means the business sees a quicker return on investment, especially for new

larger health care provider organisations. From there, improved efficiency and greater capabilities further drive a chance for savings.

When setting up a new health care provider organisation, there are inflated expenses related to setting up or installing new technology, real disruptions to the practice's daily output are also a risk. However, when it comes to Cloud computing, software or hardware-based solutions simply can't compete in terms of upfront costs. Cost is not the only benefit; there are several other benefits with the Cloud-based systems over server-client based. When providers store PMS software locally, it often requires manual upgrades and monitoring and the practice relies more on IT support. Cloud-based platforms do not face the same problems that local systems do. Besides, the Cloud-based systems can improve the practice financial situation in many additional ways by making daily tasks more simple and reliable as they have greater capabilities than server-client systems. For example, with the Cloud-based systems, patients can easily pay outstanding bills remotely and practice administrative staff can better track reimbursements. Health care providers use various PMS systems in Australia. Table 1.1 shows some of the PMS software systems that the health care providers use in Australia.

Table 1: PMS software system used in Australia

Health care provider organisation group	PMS software
General practice	Medical Director (MD), Best Practice (BP), Genie, MedTech, CommuniCare, Zedmed, Intrahealth, and MediRecords.
Medical specialists' practice	Clintel CareRight, Profile Specialists, Software 4 Specialists, Genie, Medical-Objects.
Allied Health Services	Front Desk, Helix, Practice Studio, Clinko, Hippocamp, PrimaryClinic.
Pharmacy	RxOne, Fred Dispense, Z Software, iPharmacy, healthsoft, myscript dispencing, rxone dispense.

Aged care	iCareHealth, Inerva, LeeCare, AutumnCare, Manad Plus, Acfi.
Hospital	Cintel, Zoll Medical, Alcidion, Vitro Software, Orion Health, EpiSoft, Carelink.

The fee-for-service general practitioner's practices use is a broader range of software systems in Australia. Even though health services are divided into two major groups as primary health care and acute care, health care provider organisations can be categorised into several groups including general practices, medical specialists' practices, allied health services, hospitals, and pharmacies. They all use a diverse range of PMS software systems in Australia because the functions and features of every PMS software system are varied. However, according to The Royal Australians College of General Practitioners (RACGP), in Australia, primary health care is largely delivered through two parallel systems: Medicare supported primary care delivered by fee-for-service general practitioners, and state-funded and managed community health services [25].

1.1.3 Electronic Health Record

In health care, a wide range of participants are involved in one patient's journey throughout his or her life and the patient's condition frequently changes over time. The health care providers that involve a patient include general practitioners (GP), medical specialists, allied health professionals, nurses, and pharmacists. Under allied health, again there are several different types of providers can be involved, such as dentists, dietitians, diabetic educators, medical technologists, occupational therapists, radiographers and speech pathologists. In addition to all health care providers, medical lab technicians, researchers, admin/reception staff, IT professionals, system administrators, even patients themselves are also participants or stakeholders of health care delivery. Also, patient health information includes a broader range and different types of detail. The health information provided in a patient's health record may include progress notes, past history, current medications, immunisation details, radiology images, pathology reports, shared health summary documents, specialists' letters, and referrals. That is why health care is identified as a most dynamic complex environment. For a better treatment to a patient, therefore, collective health information over the period is required to deliver the right health care at the right

time. It is, therefore, EHR systems have long been considered as an important part of the delivery of better health care services.

EHRs have been defined as information repositories for the health status of a subject of care; they usually reside on a database or other digital media [284] on the basis of EHRs contain retrospective, concurrent, and prospective information concerning physical and mental health, descriptions of the medical condition, and treatments administered to a subject of care [285, 286, 287, 288]. The benefits of the EHR systems are enormous. The U.S. Institute of Medicine explains the benefits of the EHR systems, that the systems (i) improve accessibility to health records, (ii) facilitate communication between staff, (iii) are repositories for information collected during the treatment of the patient, (iv) support continuing treatment of the patient, (v) is a repository of information for further treatment of the same patient, and also a knowledge base for advanced research and medical education [289, 290]. To receive these benefits from an EHR system, the system must be developed through the requirements and standards as structured, secured, and reliable EHR systems must adhere to standards that allow them to interact independently of the platform or technology used for their implementation [291]. The requirements and standards may be varied to state to state or country to country, wherefore developing and implementing a global EHR system faces many challenges.

Because an EHR health summary fetched from a number of EMRs, as an EHR is a summary of health events usually drawn from several electronic medical records and may consist of elements that are eventually shared in a national EHR [1, 2], there is another issue that arises to resolve, and this is system compatibility. While a large number of EMR systems are used in the sector by every individual health care provider group level and individual organisation level, developing and implementing a fully supported or compatible EHR system is a challenging task. As a result, again compatibility issue compromise the delivery of better health care.

Moreover, in defining an EHR system, the system also needs to contribute to the future of the health care services in general. In understanding and supporting the future of health care, education and research are essential. It is conceivable while the system is digitally stored rather than paper-based. Hence, *Iakovidis* [3] has described an EHR system as "digitally stored health care information about an individual's lifetime with the purpose of

supporting continuity of care, education and research, and ensuring confidentiality at all times". This definition has also discussed the confidentiality of the system.

In addition to the integration of heterogeneous information scattered over different places, it is one of the main goals of EHR [180], an online EHR system also enables patients to contribute more to their health information in delivering better health care. For example, with the Australian My Health Record (MyHR) system, patients can provide more information about their health including personal health summary (i.e. medicines, allergies and adverse reactions) and personal health notes (any concerns about the patients' health) on top of the health information that the health care providers uploaded for their patients. This additional information also provides a better understanding of the patients' health condition at the point of care for health care providers. That is another reason why the EHR systems become an important source of health information of a patient at the point of care in delivering better health care services. The EHR system is, therefore, not only providing a platform for storing health information digitally using the Cloud computing concept which also offers great promise for increasing the efficiency of the health care system but also the systems allow the obtainment of a considerable amount of health information that improves the quality and efficiency of medical care [4].

Furthermore, the growth of mobile devices used in accessing EHR systems also makes a significant impact on EHR advancement. The use of mobile devices for computing and communication with the support of wireless connections and Cloud computing plays an important role in the way of delivering modern health care services, especially in hospitals. These improved health care services enable health care providers to access the required health information of patients including pathology test results, various clinical or pharmaceutical data from many providers and their organisations. This development assists not only in providing required information faster but also the health care providers can access that information anywhere it is needed as mobility and improved availability allow health care personnel to dynamically access patient information in enhancing efficiency and information acquisition [292]. Depending on the computer and mobile devices for health care delivery, on the other hand, when systems are unavailable or failure to access on time, this impacts negatively. As evidence, according to approximately 1100 accidental deaths worldwide up to 1992, these were caused by computer systems failure [293].

Taking the EHR usage and its environment into account, it is easily understand that accessing the right information at the right time is crucial to any EHR system. For this to

happen, EHR systems must ensure seamless availability and distribution. However, the distributed nature of the information stresses the need for security requirements to be taken very seriously [181]. While EHR systems promised to improve the quality and accessibility of patient care, they also create a high risk for privacy and confidentiality of patients' sensitive health information.

When storing sensitive health information in the EHR system in a central server or over the Cloud become more vulnerable to theft or unauthorised access and the information can affect the nature of the patients. Accessing that information impacts the patients in many ways negatively and creates long-lasting effects. The impact may include, for example, an employer can access the employee's mental health conditions, an insurance company can view the client's health conditions to increase the insurance premium or even to refuse life insurance and a health care provider can access unnecessary health information to discriminate patients.

1.1.3.1 Why do we need EHR?

The EHR system improves communication among health care providers as well as between health care providers and patients. Improving communications in the provision of health care, promises a better quality of clinical services. The ability to share and exchanging health information online assists not only in providing higher quality health care for patients, but it also helps in creating significant developments for the health care provider organisations. A better EHR system allows quick access to patients' precise, up-to-date and comprehensive health information at the point of care whenever and wherever it needed. Also, the EHR systems support providers in effective diagnosis, reduce medical errors and provide the most efficient and possible treatment of care, based on the reliable information source. In addition to the easiness of distribution, the electronic version of health information also enables integration to other supporting tools in making better clinical decisions.

Another reason why EHRs become very popular for the national level is cost-efficiency. Using the EHR system, over time, promises great savings though investing in those systems that finds expensive at the beginning. A study by the non-profit research organisation Rand Corporation found that adopting the EHR could result in more than $81 billion in annual savings in the USA if 90% of the health care providers used it [244]. The expenses for

manually creating and maintaining traditional paper-based health records are very high and they lead to unacceptable delays of accessibility and searchability compared to an EHR system. The EHR allows the reduction of Adverse Drug Events (ADR) accounting for about $175 billion a year [245] and more than 200,000 cases of death a year in the U.S.A. [244]. The data from the EHR system also supports clinical researches that can improve the effectiveness of clinical trials and the medical treatment because these clinical studies could be performed quicker with many samples. Besides, disease-specific registries could be established [246, 247] that enable the option of disease monitoring facility and thus provide a more suitable solution including a new medication or treatment process to cure a specific medical condition [264, 265]. Moreover, the development of the EHR system is on the move using the rapidly growing technology. There are multiple, parallel efforts underway to modernise medical records systems for greater efficiency, improved patient care, patient safety, and costs savings [266, 267, 268]. This capability of adopting new technologies into the system promises even more imminent benefits. The availability of any EHR system is faster than traditional paper-based records and the health care providers can immediately access patient health information that is related to their care. Also, patients can take control of their health information. There are several standards that have been introduced to increase the self-protection of the EHR [269].

1.1.3.2 Concerns of using EHR

The health care sector focuses on cost-efficiency and quality of care. Both cost-efficiency and quality of care can be achieved by setting up a better EHR system. Although, the development and usage of EHR systems including Cloud concept repositories of health information promises a wide range of benefits, the lead for several concerns as well; the challenge of privacy, security, and confidentiality of the stored data is one of the major concerns. Even though, demanding privacy is a patient's right, the disclosure of sensitive health information can create severe problems for the patient. The disclosure of sensitive health information may affect the patients negatively. For example, by accessing this information, an insurance company can increase the insurance premium or an employer can change his or her status of employment. Moreover, some other high-sensitive data of a patient, such as a history of sexual abuse or HIV infection, may result in a form of discrimination or harassment. It is, therefore, identifying and addressing the privacy and security concerns of the EHR development and usage became one of the key requirements for the institutions or the government who develop and implement the system.

Furthermore, a better EHR system must provide easy accessibility of a patient's health information to the parties involved in the patient care. However, prospective privacy and security concerns increase while it provides better access for all involved parties to a patient's health record when it is needed. The increased use of EHRs shows a need for appropriate techniques to secure the health records, from both inside unauthorised access and outside attacks of a health care provider organisation. Besides, regulations such as the Australian My Health Record Act 2012 and the HITECH Act in the U.S.A. also dictate its protection of EHRs; however, these acts fail to explain precise concepts to implement this sort of protection. Additionally, in practice, providing this system's protection facilities for the EHR system is a more complicated process. However, privacy and security concerns are not the only fear in the implementation of EHR models. When the EHR shares health information among health care providers to deliver high-quality health care, the information they rely on must be accurate and up-to-date, therefore the data integrity also becomes one of the other major concerns. Ensuring data integrity in a shared environment is always challenging. There are other issues such as setting digital certificates for secure accessibility, system compatibility problems also need to address and resolve. Any EHR system that seeks to enforce record protection needs to address some important key features such as access control, self-protecting mechanism, and intricacy of access control policy [24, 30]. When applying powerful rules and regulations in the use of EHR systems, it is difficult to provide meaningful access control mechanisms to the system. For this reason, several hospitals rely on after incident audit controls rather than putting access control mechanisms in place. At the Johns Hopkins Medical Institution (JHMI), for instance, all approximately 8,000 staff members do have access to all patients' records [29]. The EHR systems should have a self-protection facility rather than the option of encrypting everything or nothing. When sharing the records among health care providers, the system needs to be self-protected rather than the whole protection of the system simply based on only transport-level protocols. Bearing a wide range of actors with varying levels of access in mind, the administration and management of access control policies in the health care sector is very complicated. Therefore, defining the access control matrix that permits which actors have access to which records or piece of information is critical and in great need of specialised tools and automation to manage the overly intricate and error-prone setting. Additionally, when accessing EHR systems online and meaningful access controls are in place, the systems also need online access control authorities to comply with it.

When the server or database where the patients' health information stored is unavailable, decisions for access control cannot be made, or the health records cannot be connected. Eventually, this will put the patient at risk. In the incident of failure of network connectivity for any reason, disaster of power infrastructure, the EHR systems that depend on these facilities turn off to be inoperative. This becomes another concern as this is exactly why a health care provider may require instant access to someone's health record. For instance, during Hurricane Katrina, in the U.S.A., much of the infrastructure medical centres relied upon was unavailable [273, 274]. That is another reason why health care providers give more importance to the health record availability in their work rather than on issues including privacy and security of the health information on the EHR. However, a consumer or patient expectation may differ to what a health care provider expects.

Taking these into account, governments change their privacy laws to adopt the initiatives. For example, the Australian Government has introduced My Health Record Act 2012 to enable the establishment and operation of the My Health Record [166]. Recently, the Office of the Australian Information Commissioner (OAIC) has also added a Notifiable Data Breaches (NDB) scheme in addition to the Australian Privacy Act 1988 [164]. Thereafter, in 2018, the Australian Parliament passed legislation to strengthen My Health Record including the following new laws [165].

- Allow people to permanently delete their records, and any backups, at any time in their lives.
- Prohibit by law access to MyHRs by anyone for insurance or employment purposes.
- Strengthen privacy for teenagers 14 years and over.
- Strengthen protections for people at risk of family and domestic violence
- Make clear that the System Operator (SO) cannot delegate functions to an entity other than an employee of the Department of Health (DH) or the Chief Executive of Medicare (CEM).
- Require law enforcement and other government agencies to produce an order from a judicial officer to access information in a MyHR system.
- Make clear that the system cannot be privatised or commercialised.

For another example, in the United States of America (USA), Health Information Technology for Economic and Clinical Health (HITECH) Act is established to convert the nation's health care records to digital formats such as EHR to improve the rapid transmission of medical information and making health care systems more efficient [210].

1.1.4 Cloud for Electronic Health Records

Cloud model provides computing and storage tasks from standalone systems into the Cloud. This concept requires resources such as hardware and software over the Internet. Cloud computing is a modern development in the digital world that has the prospective to consider Information Technology (IT) by organising cyberinfrastructures. The basic idea in Cloud computing is to move computing tasks from individual systems into the Cloud, which provides hardware and software resources over the Internet [212].

From an EHR usage point of view, the Cloud services promise even more easily accessibility for the system, that is one of the major features of the system. However, on the other hand, the sensitive health information stored in the Cloud left even more potential for data attacks. The data hackers target an EHR system rather than EMR because of the benefits and amount of data as EHR systems are massive and include nation-wide health information. With the initiation of Cloud computing, there are also more flexible services that can be offered to patients as the Cloud environment interact and adopt several third-parties software systems effectively. Another reason for EHRs deploy the Cloud concept was the speedier services and the accessibility that is another requirement of any EHR systems worth considering *at the right time* availability of the system. The government agencies that are responsible to deliver the EHR system also receive several benefits over the Cloud model including information technology's agility and consistency and achieve device and location independence. The Cloud services utilisations in the EHR systems also make for easy access for research and reports.

Cloud computing has transformed many industries, and health care is one of them. Storing medical data in the Cloud is becoming increasingly popular nowadays as the Cloud services promise users a high capacity to access its data through a range of electronic and mobile devices whereas reducing the costs and complications associated with upholding a physical storage system like onsite server-client infrastructure. Such Cloud computing facilities can be employed for eHealth platforms to provide information flow between multiple entities

such as hospitals, General Practitioners (GP) clinics, pharmacy, labs, and insurance companies [209]. Usage of mobile devices and new technology for communication such as wireless networks, 3G, 4G and 5G applications in health care increases the accessibility and allows access to relevant health information at the point of care. Similarly, standardised software makes possible the integration and interaction of highly heterogeneous software applications, reducing the time required to exchange medical records through the health care system [6]. Storing health information in the Cloud uses online rather than storing it locally on a storage device like hard drives. The Internet is used to connect and access the Cloud stored data. In some cases, the location of the server is a vital consideration in choosing a Cloud service. The Australian Privacy Principles [7] recommends for servers that include patients' health information will be located within Australia. Australian privacy law also requires that a health care provider organisation must take reasonable responsibility to ensure that the overseas beneficiary does not breach the Australian Privacy Principles before personal sensitive information including health data is disclosed overseas. Even though health care provider organisations have introduced the Cloud-based EHRs to reduce costs, the privacy and security of patients' health information become even more vulnerable because of less control a health care provider has on that sort of system.

While EHRs aid efficient communication of medical data and thus ease organisational disbursements with the help of Cloud computing [311, 312], the Cloud computing promise additional facilities over client-server model such as broad network access and resource pooling that provision of big data sets from EHRs.

1.1.5 Personally Controlled Electronic Health Record / My Health Record

Electronic Health (eHealth) means, the use of a digital form of the health records that uses modern technology to deliver health services. The World Health Organisation (WHO) defined the eHealth the combined use of electronic communication and information technology in the health sector [308]. eHealth is becoming very dominant in the health care sector. For this reason, most of the developed world has developed or is developing a nation-wide EHR system for the country. Even though cost-efficiency is one of the promoting benefits for the governments, there are several other benefits in using the system. Like other developed countries, the Australian government had also introduced an EHR system in 2012 known as Personally Controlled Electronic Health Record (PCEHR). The

PCEHR is one of the best examples of global eHealth system implementation [309]. The PCEHR is the digitally stored health care information about an individual's lifetime to support continuity of care, education and research, and ensuring confidentiality always [310].

The Australian Government has invested many millions of dollars to develop and implement the PCEHR system to advance health outcomes and reduce costs for health in the country [11]. The government also introduced the opt-in registration process for consumers (i.e.; patients) and health care providers. Opt-in means, there is an option to register. In other words, the health care provider organisation or consumer can register for the PCEHR system if they need it. However, on the other hand, the implementation of the PCEHR system has faced many challenges that eventually impeded its wider adoption in Australia and the acceptance by individuals (i.e. patients or consumers) and health care providers of the PCEHR system is inadequate [12, 13]. The main reason for the low acceptance of the system is the concerns over privacy, security, and confidentiality of the system. Addressing and resolving these concerns is very critical in the development and implementation of the PCEHR system.

After a patient's health information, which is known as SHS or Event Summary (ES) is uploaded to the PCEHR system, it is not yet quite clear who else can access that sensitive information other than the patient's usual health care provider. Besides, there are also instances where administration staff may access patients' clinical information in their daily role of the business (e.g. targeting chronic disease high-risk patients or sending a reminder for a pap smear test) [13]. The PCEHR is supported by a robust legislative framework that includes governance arrangements, privacy, and security framework and a regulatory regime. In addition to governmental PCEHR act, regulations and rules, standardisation, policies and procedures and associated strategies for the appropriate use of the system are still needed to ensure the security and privacy for every individual health care organisation. These documents should mention the users and their responsibilities in using the PCEHR system.

Subsequently, consumers want more information on their sensitive health information about how it is protected and remains confidential after storing it to the PCEHR. Consumers

have, therefore, argued that the best way to protect privacy is for consumers to have ultimate control over who has access to their records [14].

There were many privacy and security concerns identified with the implementation of the PCEHR including the accuracy of the data under patient control. The consumer's concerns are not only just about privacy and security of the system whereas it remains a priority for all users but also, they need to understand how the privacy and security mechanism works to protect the system. As a result of these concerns, the department of health called for a review of the PCEHR by setting up a small skilled professional panel including health and IT experts in 2013.

Even though the outcome of the review will be increasing the uptake of the PCEHR system, the review process also concentrated on several other concerns that the system faced over the last 15 months. The other concerns including whether the expectation of the users are satisfied, whether the development of the system is appropriately carried out, to understand the level of use by health care providers in clinical settings, any existing challenges in using the clinical settings, utility problems by health care providers, usability difficulty by consumers, activities more to fulfil the need of high-level usage for health care providers and consumers, potential incentive payments to use the system for health care providers and their organisations, issues in expanding the system for private sectors, and future directions of the PCEHR systems.

During the review process, the panel has consulted about 200 health care provider organisations and other organisation that are involved with the PCEHR development and implementation process. The panel also invited the individuals and organisations that had formerly made an official submission to the department that the PCEHR system needs to upgraded and provided responses on the development of the PCEHR. The review panel has received 86 responses and conducted many interviews across the Country [325].

After the review consultation process of six months, the panel has gathered all the ideas, suggestions and comments drawn and provided 38 recommendations to improve the system and increase the uptake by the health care providers and consumers. The recommendations [325] include renaming the Personally Controlled Electronic Health Record (PCEHR) to My Health Record (MyHR), restructuring the approach to governance, dissolve National Electronic Health Transition Authority (NEHTA) and replace with the Australian

Commission for Electronic Health (ACeH) reporting directly to the Standing Council on Health (SCoH), establishing a Clinical and Technical Advisory Committee (CTAC) to ACeH, establishing a Jurisdictional Advisory Committee to ACeH, establishing a Consumer Advisory Committee to ACeH, transitioning to an opt-out model for all Australians on their MyHR to be effective and establishing a Privacy and Security Committee (PSC) to ACeH. The Government has then carefully considered the recommendations that the panel submitted and accepted some of the recommendations including renaming the PCEHR to My Health Record (MyHR) and opt-in model to consider the opt-out model and calling firstly for an opt-out trial. More details about the PCEHR will also be discussed in Section 1.2.2.

1.1.6 Access Control in Electronic Health Record

Access control is a permission to access something, it might be a system. While an EHR containing highly sensitive individuals' health information in the Cloud, strict permission to enter into the system or access the system is crucial. It is, therefore, access control for the EHR is unavoidable. Access control is not only permitting the access to the system, but it also needs to provide a level of access for users to prevent unauthorised access and preserve the privacy and security of the system. The levels/ degree of the access control mechanism may be based on the users' purpose or role. For instance, in a health care provider organisation environment, a GP can access all clinical information including allergy or adverse reaction, current medication, past medical history, immunisation and progress notes with full read and write accesses while a reception staff can have limited access to a patient's demographic details including the patient's name, address, contact number, date of birth, Medicare number, gender, and ethnicity. Hence, a reception staff should not access someone's clinical sensitive information in a health care provider organisation. For this to happen, while all users in a health care provider organisation access the EHR system, access control must ensure the levels of access that are known as user privileges. Because the EHR system includes highly sensitive health information, these user privileges become more critical in a health care environment.

Furthermore, access control of the EHR system will be the key component of any security model that is developed for EHRs while the privacy and security issues are increasingly alarming and confining the advancement of the system. It is, therefore, while the access control provides sufficient security to preserve the privacy of the system, the access control

mechanism in place also needs to ensure accessibility for health care providers to access the right information at the right time in order to deliver better health care.

Assigning those access control mechanisms and user privileges for a health care organisation is a challenging task. In health care settings, while EHR systems provide a convenient way for doctors and other health care providers to interact with and contribute to patients' health data [185, 186] and EHRs are designed to enable effective [187] and safe [188] health care practices, health care organisations are considered as inherently complex and dynamic environments [189, 190, 17, 18]. This makes it difficult for administrators to define access control policies [191, 19]. EHR user privileges are, therefore, often defined at a coarse level to minimise workflow inefficiencies and maximise flexibility in the management of a patient [191].

Subsequently, there will be mechanisms that provide the sufficient flexibilities for users to handle these circumstances in a health care provider environment. However, the use of these exception mechanisms leads to additional density for the EHR systems. In addition, as a result, from a privacy and security point of view, the system is primed for misuse and unauthorised access.

Hence, it is clearly understood that the access control, is the baseline for information security [182] that gives permission to access and use the system. However, in health care settings, assigning user privileges cannot be organised at a user level anymore and it needs to be handled with a crossbreed method. This means, a series of structured and formal policies, models and roles must be defined [183]. With traditional access control models, there is usually an assumption that access permissions are known in advance, but in real environment unanticipated situations there may be the need to be flexible because it is impossible to predict all cases [184]. Taking the importance of a patient's health to the account, the access permissions or user privileges can be superseded, especially while a patient's health is at risk.

Nevertheless, over the last few years, there were more developments in access control research towards more dynamic, workflow-based and user-centered models [232]. However, the state of the art in existing health care systems appears to be the traditional Role-Based Access Control (RBAC) model, where roles correspond to job functions and

administration is centralised [233, 234, 235, 236]. However, there are drawbacks in using these models as they are not well-suited for the management of a health care provider environment. For instance, a health care provider needs to get a second opinion from another health care provider within the organisation. Hence, RBAC can provide a better foundation of access control mechanisms, however, with an additional capability to manage the situation like unplanned incidents and collaboration. There were also a number of developments that have been discussed on the model of *role allocation* that permits the users to give their role to another. Different types of access control methods will be discussed in Section 2.5.

In addition to access management (or access control) that determines which users or user groups have access to certain data, it also protects data from unauthorised access [167]. For the reason that a number of users have to get access, a mutual access control management mechanism can be created to represent the user groups' considering their routine activities to which specific user belongs, for example, admin/ reception staff, GPs and nurses are some of the user groups in the health care provider organisation environment. Every group can be assigned specific user rights. Further to this group based user rights, there will be an individual user right can also be assigned. Usually, the author of any record has the maximum level of rights including deletion to the specific record they created. Data and identity management in eHealth systems can be built to be patient-centred or health care-centric [168]. Based on the assigned responsibility, the models are varied. In a patient-centred model, the patient takes responsibility to assign these access rights while the health care provider organisation is responsible for allocating user rights and to keep the data up-to-date in a health care-centric model. For example, in Microsoft HealthVault (MHV) the user is responsible for data sharing [177].

The levels of access are also varied. For example, a shared health record can only be viewed (read-only) or viewed and edited. This is based on the assigned access level. The author of the health record has full access that includes read, write, edit and deletion. A custodian also can have the same type of access level. However, an interesting point is that a custodian can revoke anyone's access to the record, including other custodians, and including the custodian who granted them custodial access in the first place [177]. In this method, giving full access to a custodian is not the right option, especially considering a privacy

perspective. In access control or management, an access control policy would be achieved for health care organisations to ensure every user of the system follows the same rules.

1.1.6.1 Access Control Policies for EHR use

In order to protect the sensitive health information of patients from unauthorised access and misuse and preserve the privacy and confidentiality around the information, the health care provider organisations need to have an access control policy. This policy must define who has what access control within the health care provider organisation. The access control policy can be either internal or global. If the policy is internal, the policy must comply with the requirements, for example, Medicare or RACGP security policy and procedures. These access control policies must reflect all staff's access rights and permission levels or privileges. These access control policies should be flexible allowing for the dynamic environment of the health care sector as several users connect to the system from various circumstances. The access control policy also needs to describe the time period that every group of users or individuals access to certain resources. For instance, a patient health record can be accessed by a GP when the patient is assigned (i.e. usual doctor) to that GP and once the patient is assigned to another GP, then the previous GP can no longer access the patient record. In a health care organisation, even though the organisations trust their staff, non-authorised staff access to health sensitive information puts the whole organisation at risk. Hence, the Cloud provisioned eHealth systems should provide access to data only when necessary and protect users from unintentional errors [211].

Additionally, the access policy of a health care provider organisation should not interrupt the organisation's day-to-day activities of its staff. For example, the access control policy must define who has what access method whether read, write, delete, or print with duration, which user has access to what data, what type of accesses are assigned, with what tasks are given, in what situations and for how long (time period).

1.1.6.2 Digital Certificates for EHR use

The Public Key Infrastructure (PKI) is used to establish a secure entryway of communication to improve trust among objects. To enable this function, a superior cryptographic algorithm known as the Secure Hash Algorithm (SHA) is used in PKIs. In

health care services, PKI certificates create a gateway to communicate between different health care provider organisations securely. Human Services PKI certificate, in Australia, gives professionals secure access to online services including MyHR access and Medicare online claiming.

Some Medicare PKI certificates are designed for health care provider organisations and some for the individual health care providers. Every PKI certificate is assigned to perform different functions. For example, with the introduction of the PCEHR/MyHR in Australia, additional PKI certificates are also required to be used. The health care provider organisation that registered with MyHR receives an organisation-based PKI certificates known as National Authentication Service for Health (NASH). In addition to an organisation NASH PKI certificate, there is a health care provider individual certificate also available. This individual certificate assists the registered health care providers to access MyHR via an online portal from outside the actual registered organisation they work for. For example, a health care provider who works for an emergency department on-call where the hospital software system is not compatible with MyHR, can access MyHR via the individual certificate. The Australian Government recommended the SHA-1 and the SHA-2 technology standards in the use of digital certificates for MyHR.

Hence, the NASH PKI certificate not only performs an important function to authenticate health care organisations and health care individual who uses the MyHR system but also it protects the sensitive health information that interchange through the data encryption process while a user access to the MyHR. Should a message be intercepted by a party not involved in the exchange (i.e. not the sender or receiver), for example, then that party will not be able to read the message's contents [345]. Additionally, both health care provider organisation level and individual level PKI certificates support authentication, integrity, validation and confidentiality services of the MyHR. These activities are conceivable by allowing the users to recognise who has uploaded a health record, guarantee the information that originally uploaded is not modified in the communication channels, and confirm the information forwarded to the right person who is supposed to receive it.

In addition to the NASH certificates, the location certificate or site certificate assists a health care provider organisation in accessing Health Professional Online Services (HPOS)

gateway. This certificate also allows the organisation to communicate with Medicare securely, for example, Medicare online claiming for health care provider organisation. As a summary, table 2 below shows the type of PKI certificates and their functions to operate the MyHR in Australia.

Table 2: PKI certificate functions

Certificate type	**Major functions and examples**
NASH health care provider organisation level certificate	• Allow access to the MyHR through a MyHR compatible software (e.g.; Medical Director, Best Practice, Genie, Communicare, eCare, Fred, GPComplete, HealthMax). • Provide additional services including authentication, data integrity, validation and preserving confidentiality (e.g. by guaranteeing the original information uploaded was not modified during the exchange of the information). • Assist in sending messages, mainly clinical referrals, between different groups of health care providers securely. This service is known as secure message delivery (SMD). For example, a GP sends a referral to a medical specialist. Argus, HealthLink, Medical Objects and ReferralNet are some of the SMD well-known software system used in Australia.
NASH health care provider individual level certificate	• Use to access the MyHR web-based portal when a health care provider needs to access to the system where a MyHR compatible software system is not present. For example, a GP required accessing MyHR information when he or she is working in a hospital emergency department where the MyHR compatible clinical software system is not available. The GP simply insert the PKI certificate and visit the national MyHR portal in the MyHR website at https://portal.ehealth.gov.au/
Location-based or Medicare site certificate	• Assist in claiming Medicare online payments for the practice. For example, when a health care

	provider organisation submits a request after the provider sees a patient, the Medicare pays back the benefit amount to the organisation. Eventually, the whole or a percentage of the payment goes back to the actual health care provider who consulted the patient. • Validate HI number for the MyHR (e.g.; before uploading a MyHR for a patient, the site certificate validates that the information goes to the right patient.
Department of Human Services health care provider individual certificate	• Permit access for HPOS. The HPOS assist health care provider organisation to perform Medicare-associated functions online. For example, applying for a Practice Incentive Payment (PIP), access to immunisation details for a patient, patient verification process, MyHR registration, requesting NASH PKI certificate. • Allow a health care provider to access Health Care Identifier (HI) service. For instance, to get HI number to the organisation.

1.2 Motivation

While the introduction to an EHR system (which is currently known as MyHR) in Australia is the major force in driving the motivation in the need for the research, there are several other motivating factors that support why this research is presently essential to improve the health outcomes through a better acceptance of the MyHR system in Australia.

1.2.1 Electronic system usage growth in health care

Electronic system usage growth in the last 25 years has been very significant, in particular, the health care industry. Increasing the use of computer systems, existing faster Internet services, efficient storage and retrieval data using the Cloud, reliability of network systems, and effectiveness of distributed systems contribute to easy access to health information when and where it needed. With the support of these modern technology developments, the EHR systems have been developed. Even though the complete benefits of those systems

have not been realised yet, there have been several progressions that are existing in the system. Electronic usage in health care impacts the effectiveness and excellence of health care services. All the involved parties in the health care delivery including the patients, health care provider, and health care provider organisation are benefitted by the use of eHealth. Even though all groups of health care providers receive the eHealth benefits, the primary care service settings are in particular. For this reason, the Australian Government firstly targets the GP practices' MyHR to ensure the success of the system as the majority of the health information is stored in general practice systems in Australia.

Realising the benefits globally, the EHR systems are increasingly being developed and used in many countries. In the U.S.A., electronically sharing medical information from one facility to another has become more frequent and many medical organisations have implemented EHRs and Health Information Exchange (HIE) networks [138] and the veterans' service has begun to use HIE standards. The Canadian government has developed a nationwide EHR system known as Canadian Health Infoway (CHI) to deliver better health care services. New Zealand, England, Denmark, Singapore, and Hong Kong are some of many countries that developed a national EHR system to improve the health outcome and reduce the cost of health care delivery.

From a patient's point of view, using an EHR system, a patient can take control of his or her health information. The patients actively participate and manage their health concept, known as a patient-centred model [145, 146]. An EHR system is usually a patient-centred model that permits patients to include their health information including personal health notes, allergies and adverse reaction, immunisation and other health-related activities like exercise. The patient added health information can either be visible or invisible for treating health care providers. These control mechanisms are, in most cases, set by the patients [147, 148, 149].

Further, the perspective of easy accessibility and availability when and where it needs an EHR, usage of mobile devices become prevalent considering the effectiveness and efficiency of the system. The use of mobile devices by health care professionals, therefore, has transformed many aspects of clinical practice [150, 151]. With the advancement of technology in health care services, mobile devices have become more popular and familiar in health care settings in supporting day-to-day activities. This rapid progression in the sector leads to develop many medical software applications known as an *app* in the industry. Numerous apps are now available to assist health care providers with many

important tasks, such as information and time management, health record maintenance and access, communications and consulting, reference and information gathering, patient management and monitoring, clinical decision-making, and medical education and training [152, 153, 154, 155, 156, 157]. Mobile devices and apps provide many benefits for health care providers, perhaps most significantly the increased access to point-of-care tools, which has been shown to support better clinical decision-making and improved patient outcomes [158, 159]. One major motivation driving the widespread adoption of mobile devices by health care providers has been the need for better communication and information resources at the point of care [160, 161, 162, 163]. The need for increased availability, easy accessibility, and development of numerous quality medical software applications positively impact on the sudden amalgamation of various mobile devices use in health care settings.

In health care settings, there are enormous medical software applications (or *apps*) that have been developed and are in use. Some of them are linked to specific medical equipment that the health care providers use. For example, many medical software application systems have been developed to access the MyHR including HealthEngine, Healthi, HealthNow, Tyde and My Child's eHealth Record. Using these *apps,* once it is configured by providing verifications details, the Australian MyHR system can be accessed whenever and wherever. There are apps not only to access the MyHR, but a wide range apps are used in several areas to accomplish a wide range of activates including the clinical decision-making process, patient monitoring, time management, and medical education and training services. Table 3 below shows where and what mobile devices are being used in health care.

Table 3: Mobile device and *apps* usage by health care providers [161]

Information Management	**Time Management**
• Write notes • Dictate notes • Record audio • Take photographs • Organize information and images • Use e-book reader	• Schedule appointments • Schedule meetings • Record call schedule

• Access cloud service	
Health Record Maintenance and Access	**Communications and Consulting**
• Access EHRs and EMRs • Access images and scans • Electronic prescribing • Coding and billing	• Voice calling • Video calling • Texting • E-mail • Multimedia messaging • Video conferencing • Social networking
Reference and Information Gathering	**Clinical Decision-Making**
• Medical textbooks • Medical journals • Medical literature • Literature search portals • Drug reference guides • Medical news	• Clinical decision support systems • Clinical treatment guidelines • Disease diagnosis aids • Differential diagnosis aids • Medical calculators • Laboratory test ordering • Laboratory test interpretation • Medical exams
Patient Monitoring	**Medical Education and Training**
• Monitor patient health • Monitor patient location • Monitor patient rehabilitation • Collect clinical data • Monitor heart function	• Continuing medical education • Knowledge assessment tests • Board exam preparation • Case studies • E-learning and teaching • Surgical simulation • Skill assessment tests

1.2.2 PCEHR / MyHR introduction

The introduction of this initiative motivates more research in this area. The MyHR system is developed to improve the health care outcome to reduce the cost in the long term perspective in Australia. While the system has backed up with clear benefits, the

implementation process of the initiative faces many challenges. Increasing concerns of privacy, security, and confidentiality of sharing the sensitive health data over the Internet and storing it in the Cloud is on top of them. With the continued advancement of EHR systems and the introduction of MyHR in Australia, there is increasing concerns of privacy and security of sharing health data over the network and storing sensitive data in the Clouds [353 - Author's previous publication].

When introducing a new system to the public, people should have a better understanding of the system. The first impression is the best, clearer understanding will assist people in their decision making positively. A lack of understanding of a public system cannot be popular in the community who eventually need to use it. Also, public systems should be developed based on evidence by conducting proper researches. The research will show the actual requirements or expectations by the public to compare what the actual system is going to provide. There should not be any gaps between what the system provides and the public expectations or the need for the system. The research studies will assist in eliminating or reducing this gap. Eventually, the success of any public systems including MyHR depends on this gap. Eliminating or reducing these gaps influences the success of the system in the future. That is why, these challenges of the MyHR ultimately impede the wider acceptance of the system.

Furthermore, the public should know (once the patients' sensitive health information is stored in the Cloud with the MyHRs), who else can access it other than the patient's usual health care provider. For example, people are concerned that the government agencies including police, Australian Taxation Office (ATO) and Centrelink can access their health record if they required or any insurance companies can access their employer health records freely to make changes to their insurance premium and other aspects of it. The lack of information or unavailability of the actuality of it encourages misunderstanding in the community. In furthering these misunderstandings, the negative media also took a major part. For example, anonymous messages displayed including social media like Facebook stating that the sensitive health information that uploaded to the MyHR is freely available on the Internet. However, the reality is different from what the people hear and read. According to the new laws, any government agencies including police, ATO and Centrelink cannot access patients' health records unless they get patients' consent or court order. Insurance companies also cannot request the patients to provide any health sensitive

information concerning their employment or insurance. Also, until a MyHR compatible clinical software system where a patient's first name, last name, Medicare number, date of birth and gender recorded and then verified against the Medicare server details for the patient to establish a secure connection through the Site and NASH PKI certificates, the patient's MyHR cannot be reached and retrieved from the MyHR server.

Nevertheless, the situation is not always positive in every aspect of the MyHR and its implementation. There are real concerns in some features of the MyHR. In the MyHR current settings, within a health care provider organisation level, a patient's shared health summary and event summary that was uploaded by the usual health care provider to the MyHR can be accessed by all the health care providers in that organisation. In some other circumstances, these health records are accessible to the reception and administration staff of an organisation. This is possible because of their job role linked to the clinical information. For example, in a solo practice environment, the reception staff members need to perform multiple tasks including practice management, receiving calls for appointments and sending reminder letters for a pap test or to perform a health check. This issue should be managed with access control policies within the clinical system of a health care provider organisation. However, because of the nature of the health care organisations and its complexity and dynamic environments [26, 27], the system administrators are finding difficulties in assigning these consistent access control policies. The MyHR user privileges are, therefore, often defined at a coarse level to minimise workflow inefficiencies and maximise flexibility in the management of a patient [28]. These practices, eventually, result in the MyHR being left more vulnerable to any possible misuse from unauthorised access and intentional leakage of the sensitive health information by insiders within the health care organisation.

Additionally, the system administrators and technical staff of the system who maintain the MyHR system and deal with patients' sensitive information databases can leak that information and put the organisation in risk. This risk of leaking sensitive information impacts negatively for the whole organisation and its business reputation. Usually, the staff members who deal with high-sensitive information do have a privacy and confidentiality agreement with the organisation. However, having these agreements does not completely prevent these leakages occurring, but they reduce the risk based on the employee's professional integrity. This scenario indicates the level of risk of disclosure that the health

information in the MyHR systems faces. The research, therefore, must investigate and address these possibilities of internal abuse to prevent from unauthorised access and preserve privacy and security of the MyHR system. Understanding and addressing these concerns that are associated with the use of MyHR eventually increase the uptake and usability of the system.

There are some other concerns for the consumers (patients) over the current settings of the MyHR. Some of those concerns are;

(i) The My Health Record system contains an online summary of a patient's key health information; not a complete record of their clinical history [346]. The health care providers cannot depend on it when making strong clinical decisions for their patients.

(ii) Once the patient's sensitive health information is uploaded to the central location by the usual health care provider and other health care providers or organisation, maybe in the Cloud, in a shared environment, the information will be available for more than the usual health care provider. Until the patients take control and put necessary restrictions in the system, a wide range of parties who are involved with the patient health care delivery can access the MyHR because of the nature of the settings - the default setting is open for all providers. This means patient MyHR health information is available for all health care providers and their organisations who are involved in the health care of the patient including a pharmacist, allied health professional, nurse or medical specialist to access until the patient takes control to change the options. Also, the MyHR audit log system that developed within the system to identify who access the record or the email and text message notification that the system sends out shows only the organisation where someone accesses from, not the actual person who accessed the record. Considering a large practice environment with several staff working, this identification will become harder and the responsibility is miserable.

(iii) The MyHR system permits many external health software application *apps* to access patients' health information. The new laws that have been amended for the use of MyHR outline that these applications can access the patient's sensitive health information or the record with the patients' consent. However, unfortunately, and predictably, health apps are already securing

"consent" through obscure, standard form contracts, therefore patients might not be aware the app owner could sell their sensitive medical information to others [347].

(iv) In various countries, de-identified datasets from the EHR systems are being used for research purposes. The Australian government also, may eventually, be using the information in researches. De-identified data cannot be included in any identical data including patients' names, addresses, contact details, etc. This shows the only number and specific conditions against the population. However, the de-identified datasets can be re-identified using the current new technologies. For example [347], in 2016, the government released a data set that included information on many patients spanning 30 years. It was meant to be de-identified. IT researchers at Melbourne University quickly demonstrated it could be re-identified and linked to the individuals concerned. Such *re-identification* risk will only grow, as data sets proliferate, and tools get smarter.

In addition to these existing concerns over the system, the recent MyHR Opt-Out arrangement has created some more issues. While the global best practice or Australian federal privacy regulations recommend the necessity of consent for the use of patients' sensitive health information, the Australian MyHR *opt-out* scheme has disregarded all of these globally accepted best practices. There is an argument that part of the population was not aware of the introduction of the opt-out scheme. The people firstly should know about the MyHR and the opt-out announcement to seek more information about the system to decide whether they go for opt-out or just simply leave it for opt-in. The reality was the majority of the population does not bother or make an effort to follow the instruction to opt-out from the MyHR system, particularly the aged population. The MyHR system and its opt-out initiatives, therefore, will have national advertisement to bring to the attention of the population in the first place. This approach would have assisted people with an informed choice about the system, making decisions on the opt-out method by explaining the benefits of the system. The additional information that the government provides to the public must include both the benefits and the drawbacks, especially privacy and security concerns. This impartial attitude assists ordinary people in their decisions making and gives a clear understanding of the system. This understanding may work either positively or negatively because while the system shows its benefits, it clarifies the substantial risks in keeping their sensitive health information within MyHR. Subsequently, the public who

have concerns including privacy and security of their health information will need to take additional steps to remove themselves from the MyHR system [347, 348] in the opt-out scheme.

The following table 4 shows the background and milestones of the development and implementation of the MyHR.

Table 4: Major development stages of the MyHR

Major development stages of the MyHR	Year
Introduction of the PCEHR in Australia	2012
Review announcement	2013
PCEHR consultation process took place	2013
Recommendations released and publically available for people	2014
Legislation changes for the PCEHR adoption	2015
Renamed the system from the PCEHR to My Health Record (MyHR)	2016
Opt-Out trials in Nepean Blue Mountains and North Queensland	2016 (4 April to 27 May)
National Opt-Out	2018 / 2019 (16 July 2018 to 31 January 2019)

1.2.3 Data integrity in My Health Record

One of the other major concerns in addition to the privacy and security of the system is the data integrity of the system. With the introduction and continued implementation of the MyHR, the importance of data integrity has become indispensable. When it is sharing health information that assists health care providers in delivering better health care and to support the right decisions at the point of care, the information that shared through the MyHR must be up-to-date and accurate. The MyHR is a summary of a patient health information drawn from the clinical systems (that is known as EMR) that the health care provider uses in their organisation. Garbage in, garbage out – the information provided into an EMR must be supplied for any EHR system and the MyHR has no exception to this. Hence, the quality, correctness and contemporary of the data in the practice local electronic systems are crucial. The data integrity concerns, including loss of data, erroneousness and invalid information of the MyHR, could impact the patient care and the care-coordination

negatively. Eventually, in worse scenarios, these issues may put the patients' life in risk. If the MyHR data is worthless, then the outcome of any reports and researches that have drawn based on the system is also useless. The term data integrity covers a wide range of aspects. It encompasses information governance, patient identification, authorship validation, amendments, and record corrections as well as auditing the record [20]. It, therefore, not only outlines the data contained within the MyHR itself but also includes the security measures or controls in place. Poor security controls may also influence data integrity in MyHR systems destructively. In other words, the higher security mechanisms and control put in place for the MyHR system will ensure data integrity within the system. The absence of the safeguards for health records could reflect an inaccurate picture of the patient's health information and this will be less trustworthy for health care providers.

1.2.4 Other MyHR related concerns

Change management has also played a big role in the uptake of the MyHR system. While a consumer can use several ways to register including paper-based, over the phone, online form and in person at any Medicare or Centrelink outlets, a health care provider option was only paper-based when this system is introduced. For a health care provider, this registration process has involved many paper forms. In a health care environment, time is always money. The health care providers and their staff do not want to spend a lot of time in paper-works. Additionally, the registration, involved is a legal agreement between the principal of a health care provider organisation and the government (i.e. department of health). In most cases, the principal of the health care provider organisation is a general practitioner who works in that organisation. Hence, until the organisation understands the real benefits of the system, they do not want to spend time completing paperwork and following up for the completion of the registration process. This was the first challenge for the adoption of the system.

The consumers, on the other hand, do not have sufficient information about the new system. Even after 12 months of the introduction, the majority of the population were not aware that there is such a system existing. Furthermore, even though a proportion of the population had heard about the system, they do not know what the system is for and what the benefits are. Also, a larger number of the population had heard about the system did not

know that the system was free and no cost involved for the registration. Not too many people want to take time to register or bother about it.

For health care provider organisations, even registration and setting up the system for the organisation have faced numerous challenges. An addition to the registration process, setting up the PCEHR system for the organisation is another challenge. Once the organisation applied for site and National Authentication Services for Health (NASH) Public Key Infrastructure (PKI) certificates, in setting them up for the practices they may have faced too many technical issues. In addition to these organisation certificates, a health care provider individual should have the authority to use the system. This also involves more paperwork and technical settings. On top of everything, the health care provider needs to know how to use the system or how to upload a Shared Health Summary (SHS). An organisation is also asked to develop a policy and procedure for the registration and use of the PCEHR system. Overall, the introduction of the PCEHR system has given additional encumbrance and liability to the organisations. With the opt-in introduction, the majority of the organisations or consumers were not prepared to register for the new system.

The consequence of such decisions is that EMR and EHR systems are left vulnerable to misuse and potential abuse from insiders (authenticated employees of the institution), which ultimately can compromise patient confidentiality. Furthermore, IT technical staff or the system operators who maintain the IT systems and the databases also may access patients' clinical information. This leads to a risk of intentional or unintentional leakage, despite privacy and confidentiality agreements. However, these agreements do not eliminate leaks occurring; they mitigate the risk, based on the person's professional integrity. This demonstrates that information stored in EMR and EHR databases or the Cloud servers face a significant risk of exposure. This potential for internal abuse must be addressed. It is also important to acknowledge and investigate these challenges and shortcomings associated with the current electronic health information system and determine possible solutions to ensure its wide adoption and success of the PCEHR system in Australia.

In addition to protecting the information that is stored within the MyHR system from outside attacks and hackers, it should be inaccessible for any person that does not have the right privilege to access the whole or a part of the information. To make this worse, in some

cases, the patients provide authority for their health care providers as their delegates to access the information (e.g.; emergency level access). These circumstances can also create conflicts between legislation and the real need for health treatment. At present, it is understood that the importance of accessing the right information at the right time (that means faster accessibility) is the key to deliver better health care. A real need for the information or access to the MyHR system must satisfy both the legal and the legitimate requirements of it. There is no appropriate control mechanism to verify that status of the access to the MyHR whether it is authorised or unauthorised. It, therefore, should be an identification technique to verify the access has adequate privilege rights to do so. For example, someone who simply gets the credentials can have complete authority to perform all functions.

The threats that are identified and targeted the use of MyHR can be divided into two major groups such as outside attacks (i.e. the attackers have no access rights) and inside threats (i.e. who misuses his/her full or part of access rights). The information stored in the MyHR system must be protected from both these groups using impending techniques including strong authentication methods, complete access policies, and high-secure storage options. Even though backing up health records into scattered storage devices including the Cloud type's storage can increase the availability and accessibility of the information, this approach may create some additional security concerns. The insider threats can easily be determined, for instance, an audit log file can monitor the accesses but it is difficult to resolve because of the nature of the health care service settings. Preventing internal users who have no full access rights or privileges accessing the sensitive health information is not an easy task. Furthermore, MyHR is one of the patient-centred models. It means the patients themselves must assign access rights and privileges within the system. This is additional responsibility for patients who are not always conscious of the potential risks associated with permitting access to a third party.

Intensifying social media and social networks create new threats to privacy. The possibilities of data mining and profiling contribute to these new security threats. Using these techniques, unidentified data can be traced and matched to a physical person. While personal health information becomes a part of a social platform, privacy risks are also growing, like the ones that arise from social networks. Most of the social network users are not aware of the impact of sharing health data on social network platforms. The patients

still need to understand how their health data is managed in a situation like emergencies and the patients can actively participate and be involved in their medical treatment. The use of the social network also indicates how the MyHR can be used. The same threats that are targeted in a social network and its environment can be imagined in the MyHR system. The fact that the personal sensitive information can disclose from any unidentified data using data mining techniques demonstrates that any third-party providers who are attached to the system can be permitted to access the information in the MyHRs. The data can be gathered from several sources and be combined to create a profile for the user. Then the data can be shared among strangers' users and this may occur intentionally or unintentionally. The risks and the circumstances are almost similar in both the social network platforms and the MyHR system. These threats can be minimised with anonymisation of data that uses pseudonymisation techniques and by educating users to recognise risks [179].

The risks of unintentional leakage of Personal Health Information (PHI) have increased in the recent past. Unintentional leak of the PHI encourages any unlawful activities including medical identity theft. This allows an imposter to obtain care or medications under someone else's identity [237] as someone's PHI is an important source of identity theft [238], and has been used by even terrorist organisations to target law enforcement personnel and intimidate witnesses [239]. In the past, PHI privacy and security breaches had transpired in several domains. One of the best examples is, PHI has leaked from a Canadian Provincial Government Agency (CPGA) [240] and health care providers, through documents sent by employees and medical students [241]. There are several other instances where those leakages happened on shared environments: a chiropractor exposed his patient files on a peer-to-peer network, including notes on treatments and medications taken [242], a criminally obtained password for 117,000 medical records through a file-sharing network [243].

The change is another challenge. The health care providers need to upload updated information about a patient's health that relates to the specific visit at the end of a consultation. This update may include allergy and/ or adverse reactions, medication, medical history, and immunisation. If they fail to provide an update at the end of the visit, the information available for other health care providers is not current. Although, this issue consequents data integrity concerns, the key reason to fail to update the information to the

MyHR is the change. The MyHR is comparatively a new initiative and practice for health care providers and thus it will take some time to become in the normal practice.

1.2.5 Data privacy and security

The health care providers depend on the shared health information that is uploaded from various organisation including Medicare, general practices, pharmacies, pathology and radiology labs, and hospitals. The following table (table 5) shows the type of organisation or entity that contributes to the type of document or information to build the MyHR.

Table 5: Type of documents and contribute entity to build the MyHR

Type of document	Contributed by
Shared Health Summaries (SHS), Event Summaries (ES) and prescribed medications	General practices
Specialist letter and referrals	General practices /Medical Specialist practices
Discharge summaries	Hospitals
Supplied medications for prescription and prescription view	Pharmacies via Medicare
Medicines view, Medicare services including Medicare Benefits Schedule (MBS) and Department of Veterans' Affairs (DVA) details, Australian Organ Donor Register (AODR), Pharmaceutical Benefits Scheme (PBS) and Repatriation Pharmaceutical Benefits Scheme (RPBS) information and Australian Immunisation Register (AIR) and any cancelled vaccinations.	Medicare
Reports from pathology and radiology (test and scan results)	Pathology and radiology companies via general practice
Contact details, emergency contact details, current medications, allergy and any adverse reactions details, Veterans' Australian Defence Force (VADF) status,	Patient or consumer

indigenous status and Advance Care Plan or custodian's contact details	

The health care delivery using the MyHR, therefore, relies on a wide range of information drawn from several organisations and entities. That is why health care is known as one of the complex and dynamic sectors. The need for many types of information and having them in the MyHR to deliver better health care not only creates complexity in the use of the system but it also increases the concerns of privacy, confidentiality, and security of the information. The involvement of the sensitive information from numerous organisations and their systems and people even upsurge these concerns. This is another reason why the patients do not want to share their personal health-related information that is stored in the MyHR. While the need for important health information is vital at the point of care, limited information availability or fail to share relevant information for the care will compromise the better health care treatment. In other words, the effective usage of personal health information systems is hard to achieve without addressing the patients' privacy and confidentiality concerns [256]. Whereas better-shared information from the relevant details of a patient's health is essential to the patient's future medical, the privacy, security, and confidentiality concerns limit the achievement of it. Therefore, there should be a balance between accessibility and privacy and confidentiality requirements. In the sense of this, even though, the MyHR system enables the easy sharing and distribution of patient information whenever and wherever needed, the system must address the privacy, security and confidentiality concerns associated with the use of the system as globally, privacy has always been one of the main concerns in any eHealth systems [313, 314]. For the reason of privacy is the right of individuals to keep information about them from being disclosed to others [315] and the information that is shared as a result of a clinical relationship is considered confidential and must be protected [316].

The patients, generally, do not want to share any sensitive information with others unnecessarily except to their health care providers. The sensitive information may include mental health details, sexual health information or even drug use. This is why patients expect a strong privacy protection mechanism in the MyHR system. To make the patient's concerns worse, in a digital environment, the exposure of sensitive information cannot easily be recovered and the negative impact of it will be high for a long time in the

community. Once they shared this sensitive information with their health care providers either (i) they do not want to upload the details into the MyHR or (ii) they do worry about the privacy, security, and confidentiality of the system. Selecting either (i) or (ii) approaches, ultimately impacts their future medical treatment negatively. Not giving patients control over their private data might result in patients withholding or trying to delete sensitive medical information from their EHRs to preserve their privacy [317]. This may be a reason that the MyHR provides the patients' control in the availability of a record to a specific health care provider or group.

Additionally, a system administrator or operator can intentionally or unintentionally leak out patients' sensitive health information for any reason including revenge, profit, or other ill purposes. In the conventional privacy-preserving techniques, system administrators and operators are assumed to be trust-worth. However, this may not always, be the case. Therefore, when preserving privacy for the nation-wide health system, there should be mechanisms in place to monitor those above assumptions, situations or variations. The MyHR system must be dealt with user authentication, access control, user privileges rights, and user authorisation effectively to manage a high volume of patients' sensitive information. Consequently, there will be a need for a multi-layered security model to protect the privacy of MyHRs.

Besides, the complexity of an EHR system including the MyHR creates some other technical issues including unavailability and denial of service. Even though, having all relevant health information to the medical treatment in the MyHR, the system is unavailable at the point of care is useless. Also, due to this complexity of EHR systems, there will be more possibility for a health care provider to make innocent mistakes that can cause disclosure of a patient's sensitive health information. For example, adding someone's medication to someone else's record while opening more than one patients' records using a health care provider's clinical system.

1.3 Purpose and Significance of the Study

The transformation from the paper-based medical records to the digital version of the record (either electronic medical records or electronic health records) was significant for the health care sector. 25 years ago, patient records were on 8 x 5-inch cards and receipts

were done using the Kalamazoo system, suture material was acceptable to reuse if soaked in antiseptic solution, and the only transfer of information was by telephone or mail [1]. The environment has now rapidly changed. In health care provider settings, 98% of general practitioners now have a computer on their desk and 70% to 94% use computers to the level of regularly documenting progress notes/clinical records [2]. The clinical systems are being used to document all health-related information including allergy, past medical history, current medications, immunisations details and progress notes became widespread and it is still on progressing. An EHR provides the summary of health events that usually strained from numerous EMR systems or health care providers clinical system. Also, an online EHR system empowers not only in managing and contributing own health-related information in a consolidated approach for a patient it also prominently assists the storage, access, and sharing of patients' health data for health care providers. Furthermore, storing medical records digitally on the Cloud offers great promise for increasing the efficiency of the health care system. As a result, a national EHR was introduced to Australia in 2012 and the Government has invested multi-million dollars to build key components of the PCEHR/MyHR to improve health outcomes and reduce costs in Australia [15].

However, the initiative of the PCEHR/MyHR system faces many challenges which eventually impede its broader acceptance of the system. The privacy, security, and confidentiality of patients' sensitive health information are one of the major ones. Once patients' health information is uploaded to the MyHR, the patient is not aware of who else can access their sensitive information other than the patient's usual health care providers. In a large health care provider organisation where several health care providers working, all health care providers can access a patient's clinical information in addition to the usual provider of the patient. This access must be given for only the usual provider unless the usual provider gave access to another provider with the patient's consent.

1.4 Statement of the problem

One of the major functionalities of the MyHR system is to ensure the availability and accessibility of important health information of a patient at any time and from anywhere. In reality, the information can also be easily stored and accessed by a range of technologies including mobile devices. The technology facilitates the exchange of sensitive health information among health care providers and other involved parties. The Internet is used to upload and download health information. In the process of uploading, storing and

downloading, patients' sensitive health information must always remain protected, particularly considering legal and ethical consequences including privacy and security of the impact of the data. To protect sensitive information, proper security services must be in place. This security services and the mechanisms are essential (i) to allow access to authorised users and (ii) to protect the sensitive health data.

The unauthorised access and release of sensitive information are considered a breach of privacy and confidentiality and this could lead to the issue of public concern such as discrimination, embarrassment or economic harm [16]. The legal and ethical technological dimensions of protecting patients' privacy and confidentiality is a major concern that has not been effectively addressed in the past. An appropriate security multi-layered model to prevent a wide range of security threats is also essential.

This thesis has the purposes to research privacy and security concerns associated with storing patients' health sensitive data in the MyHR system and to suggest a suitable security method to protect the data.

1.5 Research question

The patients' privacy and confidentiality can only be achieved by incorporating appropriate security services and mechanisms in place to protect the data against being accessed by unauthorised users. Besides, a proper EHR system not only should guarantee the protection of patients' privacy and confidentiality but also assure the reliability and integrity of the information gathered by health care professionals [349]. Therefore, addressing the security of stored data, access control, user privileges is essential. This research aims to address database attacks, potential solutions for those attacks, data integrity and the importance of security in the MyHR. This research also discusses concerns with the current settings of the MyHR system. To achieve the objective of this research in the domain, the following research questions must be answered:

- *How could the storage and access of an EHR or the MyHR be supported by incorporating security services in a shared care environment?*
- *What are privacy and security concerns associated with using the MyHR or an EHR system in general? How could these concerns be addressed and resolved?*

1.6 Research approach

This research will analyse different approaches used to protect information stored in MyHRs and determine and discuss the strengths and weaknesses of those approaches. The research methodology will focus on the following stages.

(i) Investigation of the different attacks that have targeted health data in the past
(ii) Analysis of the appropriate solution for each data attack
(iii) Research of the existing access control methods
(iv) Development of the new method to protect the information in the MyHR
(v) Implementation of the new system that satisfies the need of the security controls.

1.7 Research Scope

The aim of this research is to provide a high-security model to protect highly sensitive health data in EHR systems in a shared care environment. Even though throughout the thesis, both primary and secondary use of the health information will be discussed, the main focus of the research is primary use and therefore the solution proposed will be the primary use of information.

A prototype version will be implemented to evaluate the software program specifications having been presented and discussed in this thesis. The implementation would be used to test the proposed solution in a simulated environment based literature review. Therefore, the scope of this research is to provide a detailed software program specification for secure health information stored at a conceptual level rather than to provide completely functional software with that purpose.

1.8 Organisation of the thesis

This thesis is organised in chapters and there are seven chapters included. Chapter one provides an overview of the research with emphasis on the background of the components involved, motivation, purpose and significance, approach and scope of the research.

Chapter two offers background knowledge for the research topic through related work and discussions of literature review in the pertinent topics. The literature review discussion and

analysis cover the current health care system, the importance of privacy and security of health data, other ethical and legal issues in storing and accessing health information and various challenges involved in securing health data. Key access control types, access control of the PCEHR or MyHR and previous health care database attacks are also discussed in chapter two.

The research design and methodology are discussed in chapter three. This chapter describes the research design, methodology, stages of the research. The health database security and internal abuse in database security are also discussed in chapter three. The conceptual approach and analysis including assessment and solutions for the previous health database attacks, current EHR architecture analysis, and data integrity analysis, are described in chapter four.

In chapter five, the proposed security model is analysed and illustrated with three levels of the security framework. The implementation of the proposed model is discussed in chapter six. The implementation covers the software life cycle, system design, system implementation, system testing, and evaluation. Finally, the thesis completes the conclusion in chapter seven. However, this chapter is split into two major parts such as actual conclusion and future suggestions.

Chapter 2

Literature Review

As it has been discussed in sections 1.1, 1.2 and 1.3 the background of the EHR systems, the importance of having them in the modern health care delivery, raising concerns of the development mainly around privacy and security and security mechanisms to protect the patient's health sensitive information in the EHR systems. In this chapter, all the relevant components within the scope will be discussed in detail as well as concepts of the EHR analysed.

2.1 Health care systems

A system can be understood is an abstract representation of objects or processes, a model or a natural artefact in the real world [29, 30]. Hence, the health care system should be an interpretation of an intellectual picture that outlines the major functionalities of all associated technological, logistical and administrative infrastructure of the system. The goal of the health care system is to improve the health outcome of the population in the most efficient way using the available resources to satisfy the needs effectively. Therefore the health care system can differ significantly considering several factors that influence in each country including culture, history and development level. For instance, the Australian health care system encompasses a combination of public and private health care providers' services. The funding for these services comes from all levels of government (including federal, state and local), health insurers, non-government organisations and even from individuals. The Australian Government generally contributes the funding through two national health subsidy schemes: (i) Medicare Benefits Scheme (MBS) and (ii) Pharmaceutical Benefits Scheme (PBS). In the meantime, there are other additional services and supports such as: social welfare services, regional and remote health care programs like *lifespan* and *headspace* for mental health, additional funding programs for chronic and complex conditions are also available.

The actual definition of the health care system explicates that a health care system is a collection of many resources including health labour force, infrastructure, and technology used in the system with a serviceable structure that is in place to deliver health care services to the public in a country. The analysis of the complex structure of the health care system is not part of the aim of this research; however, a broad understanding of the health care system is useful for the central topic of this research. The health care of a patient is the fundamental basis of the health care system. A proper health care system must capture, store, manage and transmit health information relating to the health of an individual and the activities of health care organisations the health sector.

2.1.1 Health Information System

Health Information System (HIS) has been utilised for collecting, processing, storing and transforming the required information for planning and decision making at different levels of the health sector to provide quality services [32]. A HIS is an intersection of health care's business process, and information systems to deliver better health care services [31]. Computer-based information systems have been commonly used in health care since the 1960s. However, in the 1990s, the purpose of research and commercial applications moved to a patient-centred data processing approach as well as through the local and regional integration of the health information system [33].

Nowadays, the central point of interest is the development of EHR to exchange important health information including medical history among health care providers to provide better health care. Haux in [33] explains, HISs are applications that collect, store, process and provide data, information, and knowledge for the provision of multiple services in the health care domain. Information is a critical element for the decision-making process in health care settings. In this sense, data quality and accessibility have become major factors for the delivery of health care. The right health information of a patient needs to be accessed at the right time in the right place for a reliable health care delivery. A good HIS system can be beneficial for health care consumers (patients), health care providers and people who manage the system (practice staff).

2.1.2 Health Record

In general, a health record is a collection of relevant facts of an individual's personal health information, including allergies, immunisation, past medical history, current medication,

and progress notes. The information is recorded by a health care provider to use that information for continuity of care. The health record can be either paper-based or electronic. The paper-based records include handwriting and computer and ICT technologies are used in electronic-based records. The electronic records may be either an electronic health record or electronic medical record.

2.1.2.1 Traditional paper-based patient health record

In the early days, paper-based patient records are used, which means information about a patient health treatment produced, stored and accessed in paper format within a health care institution. Every health care provider organisation maintains paper-based records in their convenient way. Generally, every patient has a paper-based file that was kept in a cabinet in alphabetic order. When a patient books an appointment, the file can be accessed by the health care providers. This historical paper-based record is generally referred to as a patient's health record. The paper-based patient record is still the main source for information management in daily care delivery for several reasons. In utilisation of the paper-based patient record, both as a reminder to health care providers to report events, such as the course of an illness and as a tool for communication among clinicians [34, 35]. However, the paper-based record involves mainly of free texts in an unorganised or less-organised way. Hence, paper-based records are not effective and efficient enough in supporting the clinical decisions making the process. Other drawbacks of traditional paper-based health record are;

(i) Difficult or inefficient to trace or search back a patient's historical information or retrieve relevant details.
(ii) Potential writing mistakes or difficult to understand.
(iii) Easy to misplace
(iv) The paper/writing change over time and this may result in loss of complete historical information.
(v) No back-up.
(vi) Susceptible to the natural disaster including flood and fire.

The evolution of health information systems and the development of communication and information technologies have made possible the collection, storage, retrieval and transference of electronic health information.

2.1.2.2 Electronic Medical Record

Electronic Medical Record (EMR) systems are the computer-based application that allows the collection, storage, and retrieval electronically during a patient's consultation and other times. EMR over an EHR utilises within a health care provider organisation. EMR has been discussed in detail in Section 1.1.2.

2.1.2.3 Electronic Health Record

In this Section, EHR is analysed in the literature review perspective in addition to Section 1.1.3. EHR is, similar to EMR, a digital version of patient health information that is maintained over time and may include all or most of the key administrative clinical data that is relevant to the patient's care such as demographics, medical history, current medication, any allergies or adverse reactions and immunizations under various health care providers. The EHR may also include pathology and radiology results that may be useful for the patient's future treatment.

The EHR systems empower access to health information and have the prospective to simplify the health care provider's workflow. In addition to the supports directly providing in the actual health care delivery and its associated activities including decisions making the process, an EHR system also assists some other activities including quality management and patient outcome reports that contribute to the patient health outcome indirectly.

Taking the active participation into account, the EHRs also improve the communication between patients and health care providers and this helps to develop a strong relationship between them. In the continuity of care perspective, this strengthens a relationship significantly. The actual information with quicker access when and where it is needed allows health care providers to make the right decisions at the right time – this is the primary function of any EHR system that requires it to be performed. The EHR can also improve patient care by:

- Reducing the medical errors over handwritten or paper-based sources and increase the precision and transparency of the information.

- Providing access to relevant information to make better decisions for both health care providers and patients.
- Improving information availability feature assists in reducing duplication of tests and scans and reducing unnecessary delays in providing treatment.

Several designs [169, 170, 171] of EHR systems have been proposed that especially focus on maintaining the safety of the EHR. Other real implementations of EHR systems are for example *Microsoft HealthVault* [172], *Dossia* [173] or *GNU Health* [174]. Even though these web-based EHR services are more efficient in storing health information and increase the accessibility, these depend on the patient's credentials, e.g. username and password. It cannot access information in real-world situations where patients may forget such credentials or may simply be unable to provide such information in a given circumstance [303]. For this reason, Google Health is one of the discontinued solutions [175]. According to an *official 2011 blog post* [176], the reason for discontinuation was the lack of use and impact on the health industry. Therefore, in 2013 the Google Health patient data was systematically destroyed and unrecoverable [175].

As Health Information Technology (HIT) and health care workforce grow rapidly in diversity, health care has been identified as one of the complex sectors. This is a concern because evidence suggests that complex HIT can interrupt care delivery [192, 193], contribute to medical errors [194], and expose patient data to breaches [195]. Additionally, the consequences of such incidents leads to undesirable media attention, loss of patients' trust and sanctions imposed by state and federal agencies. It is therefore critical that information systems in the health care setting are implemented and deployed in a manner that upholds the privacy of the patients to whom the information corresponds [193]. A substantial amount of attention has been allotted to avert hacking from adversaries external to the health care organisations [196, 197, 198, 199, 200]. However, the insider threat did not receive adequate attention from the research community, despite its acknowledgment as a real and growing problem [201]. This is a significant concern because evidence suggests the greatest risk to information systems stems from authorised users [202, 203, 204] because the unauthorised access to health information could lead to privacy compromise, deterioration of trust, and eventually harm [205, 206]. For this reason, health care providers have also voiced major concerns over the privacy, security, and confidentiality of current EHR systems [207]. It has also been suggested that the safety of

EHR systems could be improved by incorporating more stringent security procedures, such as access limitations and detailed audit trails [208].

Huston [257] discusses the general security concerns on implementing e-medical records and technological and administrative tools available for safeguarding the e-medical records. *Stein* [258] in his model discusses the different scenarios of EHR and highlights threats and promises. In this model, while dependability, responsibility, and privacy are considered as threats, stability, tractability, accessibility, and superiority are considered as promises. One of the major privacy concerns arises while the information is exchanged in the EHR system from one health care provider to another. *Taskforce on medical informatics* [255] discusses some issues related to the exchange of medical records among providers. *Chadwick and Mundy* [256] analysed the security requirements for the electronic exchange of sensitive documents including prescriptions to preserve the privacy, confidentiality, integrity, and availability of the system. This model also discussed the four diverse exchange concepts such as Transcript Consortium, SchlumbergerSema Consortium, Pharmacy 2U Consortium and the University of Salford Model published in the U.K.

Another approach for storing and sharing medical information is via a flash drive. The Health Key is a U.S.B. flash drive sold by MedicAlert [304]. This provides storage for medical records to keep and retrieve them when needed. However, the feature of prompting automatically the user with its contents when inserted the device (i.e. U.S.B. flash drive) option raises a high risk to patients' privacy and confidentiality. This will increasingly result in identity theft as well. The difficulty in keeping information up-to-date for this method is also one of the drawbacks. *The Band* is another proposed method presented by *Hinkamp* in which patent suggests a health system built around the smart band, which stores patients' health data [305]. In this model, network servers retrieve the health information when it needed and useful while a patient presents at the emergency department with the possibility of real-time accessibility. However, this method relays on the assumption of the patient will be carrying one when present such health services. In practicality, this is unfeasible to consider the nature of health needs.

There was another approach introduced and known as a carried-on token approach that used *rendezvous-based* access control [257]. This method rejects accessing patients' information in the EHR through the Internet. The health information is accessed through

a Global **S**ystem for Mobile communication (GSM) servers placed at any location where the information is required, for instance, in the emergency department. In terms of privacy and security, this approach is safer than the Cloud-based systems. In this method, health care providers gain access through a token that the patients provide at the point of care. Even though this approach is efficient and safer as GSM servers are decentralised and the information stored is independent of others, the need of carrying the token by the patients for the health care provider to gain access and the unavailability of GSM access points are weaknesses of this method.

Some other approaches require the use of smartphones' Internet capability for accessing web services [303]. *Kulkarnim and Agrawal* propose a health care system for developing countries based on using smartphones as tokens [306]. This is a token-based method that uses the smartphone enablers to provide medical guidance whenever the information required with the help of external hardware senses. The services that this approach provides are limited, for example, this approach is not designed to cover the emergency accesses. Another approach that presented by *Gardner et al.* [307] is known as *secret sharing*. In this method, the patients keep their health records within their mobile phones. To preserve the privacy of using mobile phones, this tactic has several user privilege levels to access health data. For instance, in addition to the combination of username and password, biometrics is also used in gaining access.

2.1.2.4 My Health Record (MyHR)

The Personally Controlled Electronic Health Record (PCEHR) or My Health Record (MyHR) is a shared electronic health summary that has been developed by the Australian Government with implementation overseen by the National Electronic Health Transaction Authority (NEHTA) in 2012. As discussed in Section 1.1.5, the initiatives face many challenges. Both health care providers and consumers (patients) do have legal and ethical concerns including privacy and confidentiality with the system. In addition to health care providers facing some accessibility-related concerns, the consumers also find difficulties in accessing their health information from MyHR. In some cases, consumers must pay to access their health information. The current MyHR system must resolve this issue and give free access for patients to access their health information for the reason of overwhelmingly the consumers want to have access to their records [80]. However, the implementation of the MyHR system needs to overcome some real concerns with the system. The option of

given permission for consumers/patients to remove the document uploaded by a health care provider is a concern for health care providers particularly. The health providers contend that the consumer should not be permitted to remove the uploaded documents. The reality is, once the document is uploaded for a patient whether it is Shared Health Summary (SHS) or Event Summary (ES), the patient can view (read-only mode) the details and the patients cannot modify any details in it because when a health care provider creates records it is turned into Clinical Document Architecture (CDA) type which is a non-changeable format like Portable Document Format (PDF) [78].

With the current arrangement of the MyHR system, the patients cannot modify the information that uploaded into their records; however, they could delete the whole record completely [81] as shown below in figure 1. The health care providers do not prefer the option their patients can remove the relevant health information that they uploaded. Once a health care provider decided that a piece of clinical information is essential and uploaded as it is important for future treatment, then why the patients should have an option to delete the whole SHS or ES from their record?. For this reason, the health care providers argue that the integrity of the MyHR is questioned and they cannot rely on a patient's MyHR.

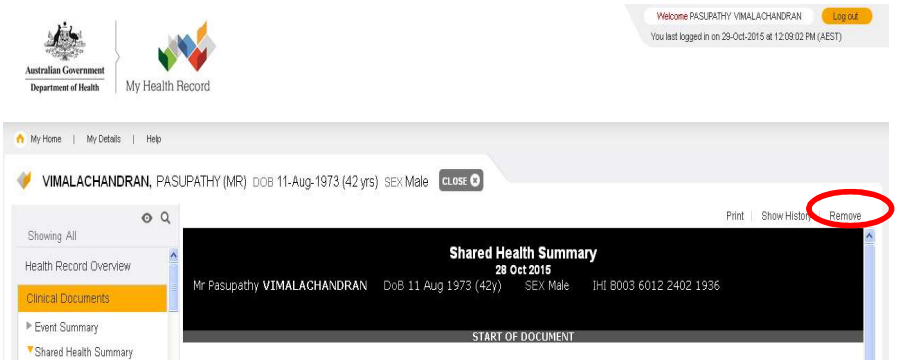


Figure 1: Option for a patient [78]

However, on the other hand, the Department of Health (DOH) argues [80], it is the patient's record and the patients should have control over the documents or information about prescribed medications or other treatment from the record [78 – Author's previous publication].

As shown below in figure 2, the patients have access and control to restrict a specific health care provider organisation from accessing one or more than one record/s from the MyHR. This raises another concern for health care providers.

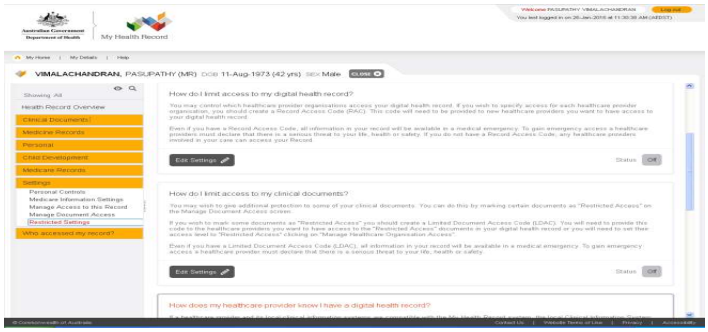


Figure 2: Patient option to give restricted access [78]

According to DOH [82], this permission offers the patients control over their records who can access it. However, health care providers fear that valuable health information will not be available for effective treatment at the point of care, particularly in an emergency or a life-threatening situation. The ability of hiding features by patients of their record, therefore, gives an incomplete picture of the health information and this leads to data integrity issues of the system. Eventually, this situation may create an unreliable position for health care providers and then compromise health care delivery. Furthermore, there is no assurance that all health providers who are involved in a patient's care will supply all relevant health information or that the information supplied will be complete.

Australian Medical Association (AMA) [83, 84] outlines that a MyHR is only a summary of a patients' important health information that supports the clinical decisions and medical treatment process. According to this statement by the AMA, therefore, a health care provider cannot completely depend on the MyHR and the usefulness of the system would be limited. The SHS or ES can be beneficial if the complete clinical information is available at the point of care. It is, therefore, important to acknowledge and investigate these concerns and shortcomings associated with the current MyHR system and conclude potential resolutions to ensure its wide acceptance and the success of the system.

2.1.2.5 Purpose of the PCEHR/ MyHR

The purpose of the MyHR is to provide a secure electronic summary of people's medical history [36] that includes health information such as past medical history, current medications, allergies and adverse drug reactions, and immunisations details. The MyHR is stored in a network of connected systems with the ability to improve the sharing of information amongst health care providers to improve patient outcomes no matter where in Australia a patient presents for treatment [37].

2.1.2.6 Architectural approach of the PCEHR / MyHR

In general, an integrated networking EHR system facilitates the exchange of medical records across the health care system. However, to make that possible, the implementation of a unified, clear and standardised architectural model is required. Various approaches have been proposed to ensure a secure, efficient and standardised EHR system. In general, the Object-Oriented Methodology (OOM) and Document-Oriented Methodology (DOM) are the two major approaches that have been used in the development of standardised EHR architecture [40].

The high-level system architecture describes the structure, linked mechanisms, their connectivity and settings, values and major features design and evaluation of the MyHR. The architecture of the MyHR also shows how all interconnected components of the system will work together to achieve its objective, for example, how the system covers a wide range of stakeholders to deliver better health care as a whole. The MyHR system has been architected using the Agency's National eHealth Interoperability Framework (NEIF). The NEIF is based on a combination of the Australian Government Architecture and HL7's Service Aware Interoperability Framework (SAIF) [38]. The NEIF is used by the MyHR system to help deliver consistent and cohesive eHealth specifications, and in this manner provides a common specification language for teams involved in working in eHealth, supporting the identification of secure and interoperable services and assisting in analysing eHealth solutions to ensure that they will deliver the intended outcome [39].

The Document-Oriented methodology is focused on developing a common and standardised architecture for different types of health care documents that can be associated

with the patient. A patient medical record contains different types of documents (medical reports, test results, images, prescriptions, diagnosis, etc.) which are associated type of service provided. The Document-Oriented Methodology is utilised by the HL7 Clinical Document Architecture (CDA) and by the Japanese Man-Machine Language (MML) [85, 86, 87, 39].

2.1.2.7 PCEHR/ My Health Record in Hospital

The health care provider organisations, in general, use EHR systems for storing and retrieving (or uploading and downloading) the patient's information when it is needed. These organisations provide relatively easy access to EHR for authorised users on-site. However, in a hospital environment, this situation is different. The patients in the hospital have no direct access to MyHR. While New South Wales (NSW) hospitals have access to the MyHRs through their EMR systems, other states hospitals (the majority of the hospitals in the country) have no access to the system. These hospitals have no immediate access to the health information stored in the MyHRs.

Even though the benefits of MyHR for health care providers in the hospital are the same as in any other health care provider organisations, access to MyHR for hospitals is very complicated than other health care organisations. There are many reasons behind it for this complexity. Software compatibility is a major concern as they use various software applications and making them compatible with the MyHR will be a difficult process. To increase this difficulty, furthermore, hospitals are state funding organisations and the systems they follow contrast. Access to patient information must be done discreetly and must comply with some corporate policies such as the rules stipulated in the HIPAA Act [300]. Granting full access for health care providers to access the patients' MyHR health sensitive information will give any health professional full access to a patients' EHR may pose a potential law violation and create privacy and security risks. A study analysing whether or not different health professionals will comply with the information assurance policy of their respective health clinic reveals that as many as fifteen compliance factors are involved in such a decision [301, 302]. Providing limited access for a certain period for the providers in the hospital would be a solution in preventing the privacy and security concerns within the hospital settings.

2.2 Security and Privacy of EHR systems

With the support of modern digital technologies including the Internet and the Cloud services, an EHR system will be the key enabler in the health care sector by;

(i) Enhancing the quality of patient health care,
(ii) Increasing patient active participation in their care,
(iii) Reducing medical errors including human errors and handwriting,
(iv) Improving practice efficiencies and
(v) Saving time and cost.

The complexity of such EHR systems, however, increases many privacy and security concerns. The security and privacy concerns with EHR systems are, eventually, associated with a broader range of ethical and legal issues. The modern EHR systems encompass extremely sensitive and personal information regarding not only health history but also the delivery habits, sexual orientation, sexual activities, employment status, income, eligibility for public assistance and family history of a patient [41]. Hence, protecting EHR systems are not only for technological requirements but also for ethical and legal requirements. Preserving patients' health information in EHRs is crucial because any unauthorised access and release of the personal information contained within an EHR could cause harm to the private life of the patient [42, 43]. Furthermore, even though preserving the sensitive health information of patients is a basic need of the EHR system development, the implementation of such security and privacy measures also becomes a challenging task over time. The secure access and storage of electronic health information is required to not only protect the exchange of data but also needs to ensure that the information is disclosed only to those who need access. Consequently, both security services and mechanisms are essential for allowing access to authorised users as well as for protecting sensitive medical information during the exchange of data [44]. On the other hand, high-security measures may lead to system unavailability and inefficiency issues. Therefore, defining the correct balance between security requirements and the availability of information is a critical goal in a complex environment such as health care [45].

Compared to other sectors, the concerns over privacy and security are very high in health care as they do contain highly sensitive information, for example, the EHR. Therefore, the privacy and security options of the EHR systems must be considered carefully. The rapid

growth of middleware technologies encourages health care provider organisations to use various software applications and systems to make their job easier. Even though such systems are increasingly used in a wide range of activities including patient management, decision making support tools and billing, the information stored within the systems are stated as highly confidential and required additional access control mechanisms. Because of the nature of the system including the information stored over the Internet and the Cloud, there is a significant level of threats from hackers and malicious software. It is, therefore, access control levels and user privileges should ensure secure access to the EHR system in a health care environment. These access rights and user privileges must comply with the access control policy that satisfies the national standards.

2.2.1 Australians' Privacy Concerns

The decisions of when, where, from whom and what type of medical treatment is delivered, the privacy and confidentiality of the health record influences significantly. Nowadays, the privacy of sensitive information (i.e.; health data) becomes a serious concern with the shared and distributed systems including social network platforms and EHRs over the Internet. The introduction and rapid advancement of social network platforms may be one of the reasons why this concern becomes a major issue. The concern, eventually, affects the flow of health information for health care providers to access and use to deliver better health care.

While the privacy concern is a common issue globally, the degree of concern is varying from country to country. The concern depends on the level of priority that the public put in it. For example, the level of priority the public put in for privacy concerns in Australia is different to this level in Indonesia; even this concern would be very low in Ethiopia. There will be many reasons set this level of concern for a country. Available services, level of economy, education, and awareness, advancement of health care, communication development, lifestyle, and culture are some of them. It is, therefore, important to conduct proper research to identify the potential issues including the privacy concern with the EHR system nation-wide for a country. Similarly, in Australia also, appropriate researches would have performed before the introduction of the MyHR system. Even though there has been no research on this topic done before nation-wide, New London Consulting (NLC) has surveyed in Australia. This survey results and the analysis will help the importance of

privacy and confidentiality in Australian communities as the privacy and confidentiality concerns do impact MyHR implementation in Australia. Some of the important results from this survey [18] are analysed in the following table 5.

Table 5: Australian Privacy Concern – the survey result summary

Survey results [18]	Analysis
49.1 percent of Australian patients indicated they have withheld or would withhold their health information from their health care providers if the health care provider had a poor record of protecting patient privacy.	It is obvious that the patients trust the health care providers; however, if they come to know that their health care provider organisation does not take adequate steps to protect their sensitive health information, they will leave from the organisation. This action will affect the organisation business and reputation negatively. This simply shows that about half of the population in Australia do have serious concern over the privacy of their health information.
38.2 percent stated they have or would postpone seeking care for a sensitive medical condition due to privacy concerns.	Postponing medical treatment will put the patients' health in risk. The privacy concerns, eventually, affect the delivery of health care.
97.1 percent of Australian patients think health care providers have a legal and ethical responsibility to protect patients' medical records and private information from being breached.	Almost all population trust their health care providers and the organisation and also protecting the sensitive information is their obligation.
59.1 percent of Australian patients stated that new and stronger laws are	The majority of the population in Australia believes that the current privacy laws are not adequate to protect their sensitive health information. They

needed to guarantee the privacy of patient information.	also realise the need for new laws to prevent the current threats that they face presently.
43.5 percent indicated they would seek care outside of their community due to privacy concerns.	This simply shows the level of concern the Australian people have and just below half of the population are happy to travel significant distances for preserving privacy. In other words, they don't mind the cost involved in it – they give priority for privacy than the cost up to a limit.
4.9 percent of Australian patient respondents indicated they had been alerted or discovered on their own that their medical records had been compromised.	A significant number of patients have had experience in the privacy breaches or directly affected by this breach. This number simply shows the occurrence and possibilities of the breach. In some cases, the patients may not aware that they have had affected. Therefore, this percentage might be higher than 4.9.

The health treatment for patients in modern health care settings is utterly information-based and any resistance in the free flow of the health information between health care providers and patients ultimately compromises the patients' care. In conclusion, the Australian population believes protecting their sensitive health information is the responsibility of the health care providers and hospitals. The trust in their health care providers will last until a substantial breach happens with a provider or in the organisation. Once they hear a major negative reaction for privacy violations or any breaches story from their health care providers or the organisation, they move to another health care provider or an organisation who responses positively or where they believe that a proper control put in place to protect the privacy of the health information.

The research and analysis survey conducted New London Consulting involves legal and ethical responsibilities and with the following findings:

- There will be more positive activities to take to protect sensitive health information by the management of the health care provider organisations and hospitals.
- The health care providers should monitor on regular basis who else accesses the patients to identify unauthorised access to their patients' sensitive information.
- The Australian government also needs to take necessary actions to protect the privacy of health information including making availability of the information in which health care provider organisations and hospitals have had privacy breaches of patients' health information.
- Any privacy breaches will damage the reputation of those organisations or hospitals.
- The reputation of the organisations or hospitals impacts on the decisions where the patients seek for their health services.
- The poor management of sensitive information will be the main reason for privacy breaches.
- The patients seek health services from another provider organisation or hospital if they discover there had been privacy breaches with their current organisation where they go for health services.
- The current privacy laws are inadequate to protect the present risk of privacy breaches or they are not properly enforced.
- The additional required enforcement of privacy laws and the introduction of best practices can provide a better outcome in protecting privacy.

The majority of the population who were affected by the privacy breaches have suffered and faced negative consequences of the breach. The consequences include the health sensitive privacy is a public issue and the victim will be a subject matter in the society. The consequence of the breaches also leads to some other serious concerns within the system. For example, the breach can lead to adding incorrect information to the health record, identity theft, use sensitive information to any lawsuit that is against the victim. These types of activities will affect patients seriously.

This survey also revealed the benefits of such EHR systems including better accessibility amongst health care providers, keeping the information current and the patients' involvement and contributions in their care. The majority of Australian patients also think the health care providers should effectively work in preserving the privacy and ensuring

confidentiality by taking necessary actions including quick response in providing details for patients who else has accessed the health information other than their usual health care provider, resolve any privacy breaches effectively in a timely manner, making more awareness of the breaches and patients privacy concerns, ongoing monitor who else access the health information, and improving communications with patients in this regard.

This survey also has revealed the tasks that their health care providers can take to increase their level of trust on privacy are;

- Setting up monitoring services to prevent privacy breaches around the MyHR system.
- Providing education and training to all staff on how to protect the information and follow the privacy laws.
- Encrypting the health information before storing it.
- Investigation any suspicious data breaches immediately and effectively.
- Improving communications between the providers/organisations and patients on the privacy breaches.

Even though further academic and industry research is required to recognise the real impact in a community including emotionally, financially, professionally influences to the patients who have experienced the privacy breaches, the above survey findings reveal the importance of the privacy, security, and confidentiality of health information and in the EHR systems including the MyHR. From these findings, it is easily understood why Australians' MyHR system uptake was very low and the need for a high-security system for the MyHR to preserve the privacy of the information in it.

2.2.2 Cloud Computing Security Concerns in Australia

While the Information Security Forum (ISF) indicates that the risks of using the Cloud services for personal data can easily be managed, the reality of the risks and its effect are significant and cannot be always rectified. ISF is an international, independent information security body that considered as the world's leading authority on cybersecurity and information risk management. The privacy concerns over sensitive personal information such as health become even more serious and complicated with the Cloud-based systems. Organisational pressure to take advantage of the Cloud-based systems should be matched by equal eagerness to understand and manage this higher-level of risk. The decision to use

the Cloud-based systems should be convoyed by an information risk assessment that has been conducted precisely to deal with the complications of the Cloud systems, the data that will be stored in the Cloud, associated privacy regulations and of course the needs of the business. It should also be reinforced by business processes that ensure the required protection of the system. If not, the identified pressure to implement the Cloud services will increase the risks. The risks, eventually, fail to comply with any privacy legislation, particularly when operating across multinational borders.

The security arrangements offered by the Cloud services, and the risks that need to be managed, should be assessed individually before a decision to accept or reject a particular Cloud type and service combination is made. An organisation should use the combination of the Cloud type and service as a basis for considering the information risk; therefore, it can be appropriately managed. Cloud-based systems are common in a modern part of the business landscape because they can be cheaper, quicker and easier to deploy than internal IT systems. For services and businesses including health care, the promise of reduced costs from scalable IT services provided on demand is extremely attractive. This is one of the main reasons for the rapid uptake of Cloud-based systems. The attraction is especially acute during a prolonged economic downturn as organisations look for opportunities to outsource non-core aspects of their business.

The ISF's latest report [350] on data privacy in the Cloud discusses an outline of privacy as a notion and clarifies Personally Identifiable Information (PII), together with the demands usually placed on organisations by privacy guidelines. The report also provides further details on the development of the ISF Privacy Framework to address Cloud-based privacy issues, allowing organisations to implement the privacy safeguards and best practice strategies to an organisation and defines the activities required to attain privacy compliance when using the Cloud-based systems. The data privacy concern increases when using the Cloud services because of the risks in the Cloud services are very complicated. The lack of understanding and knowledge of the risks associated with it, the uncertainty of the actual information sites, options for easy fusion, indistinct state of future accessibility and storage of the information and unknown privacy policy and procedures of the services also make the Cloud-based systems more complex.

In terms of privacy and confidentiality concerns and its mechanisms, the easier accessibility of the information is one of the major obstructions to the development of the Cloud and its wide acceptance by health care services in Australia. The information stored in the Cloud means, the settings and controls of the services rely on the Cloud vendors and their privacy policies. For instance, if the information is stored offshore sites and those sites are located in some countries where the privacy laws are weaker than Australia, then the risks of this privacy concern should be considered very seriously. In other words, there are concerns for Australian health care organisations and services bearing in mind when they decide the Cloud options. Storing of any sensitive health information in the Cloud, constantly consequents in an expose of the sensitive information offshore and this elevation great concerns for the patients as to whether or not they have sufficient relevant information or consents available.

Even though the Cloud services increase the fear of privacy concerns, in reality, the level of privacy concerns over the Cloud services are not always high. For example, the IaaS type of Cloud services does not generally transfer the stored information to a third party or the vendor. For this reason, the privacy concern over this specific Cloud model will be lower. Therefore, the type of Cloud service options is also needed to considered and understood in the decision-making process of it. There are several kinds of Cloud-based facilities and options available to a health care organisation and every individual plan of the Cloud type and service provides a diverse variety of advantages and privacy risks to the organisation. The combination of each certain Cloud service forms a Cloud-based model and every different model has its benefits and risks. Three types of major Cloud service models are available.

1. Infrastructure as a Service (IaaS) model offers its users to access the computing resources including servers, storage, and networking options. However, the organisations have to use their platforms and software applications within the infrastructure provided by the service provider. In this model, the organisations pay IaaS on demand rather than purchasing hardware infrastructure. This model also assists in saving the front-cost of purchasing hardware requirements and allowing the virtualisation of administrative responsibility. The privacy and security, technical complications and the increased vulnerability are major issues that have to be addressed. While it is remotely managed, assigned the management of the information to service provider vendors and the consumer organisation

controls of the operating system and software applications, the risk and concerns that connected to this model are high. Amazon Elastic Compute Cloud (EC2), GoGrid and Rackspace Cloud are some examples of well-known world-wide IaaS models.

2. Platform as a Service (PaaS) provides its users with a complete physical computer hardware and software environment. Using the infrastructure services, the users are also offered other facilities including managing, developing and supplying various applications and tools including in health care. The package of prebuilt components also assists the customers to customise and assess their applications. Ability to encrypt sensitive information including patients' health record is the major advantage of this model. Allowing health care organisations and government agencies to develop the required features of the Cloud without distressing about basic infrastructure of computer hardware and network connectivity, providing necessary security and backups, and facilitating the option for remote teamwork environment are some other key features of PaaS model. Even though this model is secure, the system performance makes slower accessibility than the other models, because of the data encryption process that involved with it. Examples for PaaS are google app engine, force.com, and the Microsoft Windows Azure platform.
3. Software as a Service (SaaS) Cloud computing delivers users with access to software applications. The user organisations do not purchase and install software applications to their local devices and they can be accessed remotely from the service providers' through the web. With some service providers, there is a specific Application Programming Interface (API) to access SaaS. This subscription model offers software applications to store and analyse the data. The user organisations do not worry about managing, installing, and upgrading software systems as these are the responsibilities of the service providers. The other benefit in this concept is that the required resources can be increased or decreased considering the need of the user organisations. The efficiency of faster accessibility is a strong benefit as the users can access the system from anywhere in the world using any internet-connected devices including mobile phones. As SaaS uses a password to access the system, there is a strong need for password management policy and procedures for the user organsiations. Otherwise, this model will be more vulnerable to unauthorised access. For example, SaaS vendor services include Customer

Relationship Management (CRM), Google Gmail, Microsoft Office 365, Microsoft Exchange Online, and Microsoft SharePoint Online.

The Cloud models are also categorised based on Cloud deployment. For example, public cloud, private cloud, a managed private, community cloud and hybrid cloud. While the public Cloud shares the infrastructure with several organisations through the Internet, private Cloud services hold the dedicated infrastructure and services within the organisation or offsite.

In Australia, both Federal and State Governments enforce privacy laws to preserve privacy. The Federal and State laws concerning the health sensitive information and health record that dealt with health provider organisations and the businesses will require a confirmation from the Cloud services vendor to satisfy some further assurances on privacy and security, considering the importance of privacy concerns. In general, the Cloud services concepts are fundamentally accepted by the Australian's privacy laws or with the process of protection of information and security. This does not mean, the Cloud services raise privacy concerns in health care services. The Australia Privacy Principles (APPs) under the Australian privacy act that standardise the gathering, storing, usage and expose of personally sensitive information. If the service is hosted overseas, then the Australian patients are concerned about the potential access to their data by the overseas government agencies. With the managed services or SaaS model where the Cloud service vendors have a strong active responsibility in managing, storing, and processing the sensitive information like health data originally gathered from or held by the patients, then the service providers have more accountability under the privacy law in place in Australia. Similar to other IT services, the use of Cloud services also increases a range of privacy, confidentiality, security, regulatory and other technical concerns that need to be wisely addressed and managed. Though, from a privacy point of view, the ethical and legal issues that arise about the Cloud services are the same as the concerns that ascend in the settings of outsourcing or offshoring the ICT service models. It is, therefore, crucial that the legal consultants of the health care provider organisations completely understands the environment of both the Cloud and privacy to adopt the necessary legal protection measures in the agreement between the user organisations and the service providers.

Hence, Cloud computing promises many potential benefits including effective and faster accessibility, cost efficiency and better business outcomes for Australian businesses and

government agencies including in health care services and depositaries such as MyHR. In the meantime, given the fact that the information is stored over the Internet, information privacy and security risks are also increased. The promise of better accessibility of the Cloud services, on one hand, makes the EHR more efficient in its operation. However, on the other hand, this ability increases the privacy, confidentiality, and security of the system. The risks with the Cloud services vary subject to the sensitivity of the information that is kept or managed and the type of the Cloud service provided. Developing a risk assessment and disaster management plan would be beneficial for the health care provider organisations in making an informed decision respectively to verify whether the Cloud services meet the business objectives with a satisfactory level of risk and to monitor the ongoing risk and recover from any disaster that may occur while using the Cloud services. For a health care provider organisation, the Cloud service option must also be addressed and guaranteed the availability of data, protection of sensitive health data from unauthorised access and management of security controls.

For Australian businesses, the Defence Signals Directorate (DSD) [89] has developed a list of questions that need to be walked through by the management and system administrators while the business is making decisions on the Cloud services including best practice to identify and manage associated information privacy and security risks. Especially, the risk assessment needs to seriously consider all related possible risks when offering sensitive health information and its control to a third-party. These risks will upsurge if the Cloud vendor controls offshore or overseas. The DSD highly recommends Australian agencies and businesses to elect either a locally owned vendor or an overseas-owned vendor that is located in Australia and stores and manages the sensitive information only within Australian borders. The overseas-owned vendors working in Australia may be subject to overseas laws such as an overseas government's legal access to the sensitive information detained by the Cloud service vendor. The Cloud computing concept as a distribution model for IT services is defined by the National Institute of Standards and Technology (NIST) as *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* [90].

2.2.2.1 Cloud computing Risk Management

The user organisations are, eventually, accountable for the privacy, security, and integrity of their data, even though the data is stored, managed and maintained by a Cloud service provider. For this reason, the user organisations need to ensure that the information provided to the service provider is secure. The user organisations should confirm that the Cloud provider has sufficient and effective security mechanisms put in place to protect the privacy, security, and integrity of the data. The user organisations also need to collect as many details as possible about the security mechanisms that the Cloud service provider put in place to create an effective useful agreement between the user organisation and the service provider. The agreement should also include the details of the provider's hiring process, the level of security required and the right to request an audit report when it is needed. In the case of the user organisation that decides to use the Cloud provider who is located overseas must consider demanding the service provider to create a guaranteed commitment to comply with the local privacy and security requirements. In a Cloud environment, it is essential to encrypt the data before stored in the Cloud considering the nature of the settings as the shared data is together with the data from other users. The user organisation should, therefore, confirm the data stored in the providers' servers are encrypted and used proper user access and monitor controls. In particular, these controls are vital in privileged users' accounts.

To practice the best preparation for the Cloud services, a risk management process is imperative. The risk management process must balance the benefits of Cloud computing with the privacy and security risks related when the user organisations provide complete control to a Cloud service provider. The risk assessment also should contemplate the service options given by the service provider to satisfy their reputation, privacy and security controls in place, plan for business continuity, data exchange process, and data store and process procedures. The agreement between the user organisation and service provider needs to address the security risks mitigation process, user access accounts, and user rights; the security controls details to protect the sensitive data. The business continuity plan discusses that the necessary actions and steps need to be taken by the user organisation to protect the data to continue the business or service, after an event of disaster occurred. The user organisations need to evaluate the options of the service providers' business continuity

capacity to make sure they can meet the requirements described in the service level agreement.

There are several components that must be discussed in preparation for a better risk assessment protocol. These components may include:

- The efficiency of the security mechanisms
- The technical architecture of the security mechanisms
- Details of preserving data integrity process
- Details of the data encryption process
- Business stability
- Intellectual property
- Auditing controls

The risk management process also needs to identify the associated risks with Cloud usage and implement potential control mechanisms to manage or mitigate the risks. To achieve a proper risk management process, therefore, better communication and transparency between the user organisations and the services providers is required. The user organisations must know precisely what features are covered in that service. For example, the framework that they develop also should be effectively integrated with ISO/IEC 27001 compliance. The user organisation may request a copy of the statement of applicability, external auditors report and the conclusion of a recent internal audit report to evaluate the process. An addition to a regular review of the assessment, external independent security companies can also be invited to perform a regular external vulnerability risk assessment.

The Cloud concept promises the user organisations a cost-effective, flexible option and opportunity to continue their business. However, deciding a Cloud computing solution without proper investigation and knowledge of the technicality of the service can create serious privacy and security concerns. Utilising the Cloud service with the required level of existing protection mechanisms provide more benefits to the business or service including in health care. In the identification process of such privacy, security and integrity protection mechanisms, (i) developing a methodical approach to address policy and procedure in the selection of service and its providers, and (ii) seeking legal advice during the development of the agreement and its requirements are essential. The knowledge and better understandings of the risks associated with the Cloud services for the user

organisations help to achieve the objective of the business by managing and mitigating the risks in the dynamic and growing environment that is likely to become a more widespread model in the future.

2.3 Ethical and legal issues in storing patients' data in the Cloud or EHR systems

While the EHR systems promise several benefits for patients and health care providers, there are unsolved ethical and legal concerns that affect the widespread acceptance and use of the system in Australia. Therefore, the ethical and legal issues related to the usage of the EHR systems need to be seriously considered and addressed to ensure the adoption and use of the system. This need becomes even more extreme with the introduction of the MyHR in Australia.

2.3.1 Ethical issues

A key feature of any EHR system is the competence of easy portability and accessibility. However, the improved portability and accessibility of the EHR systems raise several ethical questions. The ownership of protected sensitive health information [46, 47] is one of them. The accountability of preventing sensitive health data and informing patients of the possibility of privacy breaches need to be accomplished by the health care providers. The patients are also concerned with the increased threat of unauthorised protected health information disclosures that may occur in the EHR system. These concerns by the patients may be valid because there are several incidents that the EHR vendors have sold de-identified data to third-parties. For example, *Cerner* and *Allscripts* (formerly *Eclipsys*) have sold their de-identified copies of the patient databases to pharmaceutical companies, medical device-makers, and health services researchers [48]. The de-identified data can frequently be re-identified using freely available exterior data sources [49]. For this reason and other related concerns, many patient privacy support groups and some media groups are not prepared to trust the current EHR systems. Possibly, the key ethical problem is whether the for-profit secondary uses of data are appropriate and justifiable, and if so, what privacy safeguards should be employed [50].

In some cases, these security and privacy breaches raise multifaceted ethical and legal issues on the suitability of present methods to address those issues. For example, the MyHR system uses audit logs as evidence to identify the organisation that intentionally accessed

the patients' health records without the patient's concern or permission. Keeping this in mind, obviously, the implementation of the MyHR in Australia also is raising some other additional ethical issues, such as;

(i) Who will manage the data aggregation
(ii) Who will verify, validate and analyse the data
(iii) Who will have access to the data
(iv) To what limit the health care providers can depend on the data that stored in MyHRs.

Many ethical dilemmas surrounding the security and privacy of electronic information are unresolved [51]. With the increased availability and accessibility of the EHRs, the health care providers must be careful to maintain the rights of adolescents in light of their parents' proxy access to their data [52, 53]. While adolescents are permitted to protect their sensitive health information from their parents if they need and consent to get medical treatments for some sensitive medical conditions in which a need for parental contribution may impede the care, consent to other therapies still requires parental involvement [51]. Taking this ethical issue into consideration, the Australian government has changed the law for MyHR to access Australians aged 14 to 17 years old which means from the age of 14, you can choose to take control of your record and decide who sees your information. When an adolescent turns 14, they must naturally permit for their parents to access their sensitive health information, however, now the parents can register their children for a MyHR and possibly can also access and control it until they reach age 18. In reality, for an adolescent, other than having an unconnected personal MyHR, it is not certain how the separate health record will limit for their parents in accessing the sensitive health information from them. It also needs to be clarified that the age limit for the health care providers to transfer their controls of the MyHR to an adolescent, especially when they reach parenthood.

While the number of health care provider organisations that participating in the MyHR systems is growing, the ethical concerns associated with the requirements to preserve the patients' privacy and data integrity is also increasing. The concerns postures significant barriers to the adoption and use of the MyHR system. This concern has, eventually, resulted in a minimum acceptance and satisfactory level of the system. A nation-wide debate involving all stakeholder groups needs to be considered to address all potential ethical and legal concerns of the MyHR usage.

2.3.2 Legal issues

The implementation of the MyHR in Australia, ultimately, offers rapid computer access for the health care providers to more than a single medical record from a health care provider organisation. Even though the initiative addresses the longstanding concern related to missing or losing of clinical information with the paper-based system [54], there is no statute or precedent to address the extent to which clinicians are responsible for reviewing information in an integrated EHR that contains data from many sources [55]. In some cases, the health care providers presently realise that it is difficult to review the complete health information held in a record within a reasonable timeframe. Additionally, an EHR system including MyHR introduces many additional liabilities for health care providers [56, 60, 61]. The EHRs can store virtually unlimited amounts of perfectly legible and instantly accessible records that include nearly every aspect of care regardless of where or when it took place, all of which are *discoverable* [57, 58]. The health care providers who miss critical information that directly affects medical treatment and the decisions while reviewing the EHR or MyHR could be liable for negligence because *the fact in question was likely just a few clicks away* [59]. The health information stored for a patient in a clinical system of a health care provider organisation must be reviewed and uploaded into an EHR or the MyHR system. The health information that needs to be reviewed may include allergies, adverse reactions, current medications, past history, and immunisations details. The information must be reviewed for the state of its accuracy and conversant. This requirement will ensure the providers' legal responsibility and accountability towards the MyHR initiative. There may be audit controls where it can be identified whether the health care providers have reviewed the health information or not before uploading an SHS or an EV to a patient. Furthermore, the problems regarding usability, quality, and reliability of currently available EHRs bring about complex legal ramifications [62, 63, 64]. To enhance the current MyHR's capabilities and efficiency, and usage, the health care providers must freely report the privacy, security and safety concerns without fear of accusation. The complete the prospective solutions that may propose for MyHR must cover a wide range of aspects of the system including the major functionalities, usability, efficiency, clinical decision support, accessibility, and potential system outages [65, 66, 67].

In a shared care setting, the delivery of health care services becomes a multitasking activity in which the collaboration of several users is required not only for delivering health care but also for keeping the health records secure by preserving the privacy and confidentiality

of the sensitive health information [44]. Besides, access to health data repositories for either primary or secondary purposes has become an essential functionality of modern health information systems. The security and privacy issues have reached the public concern, especially considering the variety of users that store and access medical data could provide and the personal, legal and ethical effects that the unauthorised release of information could have [68].

2.4 Challenges in implementing the MyHR in Australia

The MyHR system is a relatively new initiative in Australia and there have been no many kinds of research done in this domain before. To ensure the effective implementation stage of the system, the challenges need to be identified. A proper investigation is required to find the challenges including practical issues to make the system success. For this reason, this component is a key to the research and requires more attention.

In health care delivery, the availability of the information is critical in the provision of integrated health care services. However, the availability of information should be distributed under a secure environment wherein the privacy of information is guaranteed. To preserve the privacy and confidentiality of sensitive information, access to patient's data should be carried out under the principles of relevance and need-to-know [69]. As already been discussed in section 2.2, with the increased security and privacy measures, it directly affects the efficiency, availability, and accessibility of the EHR systems. Therefore, the right balance between the security controls and the process of maintaining efficiency or availability or accessibility is the key to the MyHR implementation. The availability of the information means a certain level of accessibility of the information upon request from a user. A security breach poses a risk to protect the privacy, security, and integrity of the EHR system and to offer consistent health information in the provision of health care. The privacy, security, and integrity of the information are not only guaranteed by incorporating additional security mechanisms within the system or for securing a communication channel, but also by ensuring that an authorised user only can have access, add or alter stored data [70]. Preserving the privacy, security and confidentiality of the distributed sensitive health data in a shared environment becomes a challenge in any EHR advancement. The risks identified to preserve the privacy, security, and confidentiality of the system can be divided into two groups. The first one is, the threats identified form outside of the organisation that breaks the network settings and steal the information over

the Internet and the second one is the people inside the organisation intentionally or unintentionally access the health information. Even though the first one appears more precarious, in reality, the cause of the second one is more frequent and difficult to manage with. According to one Forrester study, 80% of data security and privacy breaches involve insiders, employees or those with internal access to an organisation, putting information at risk [5]. In a shared environment, controlling who is getting what user rights to access which information becomes a difficult and time-consuming task within an organisation. Furthermore, the trust between the employees makes softer and more flexibility in the workplace also contributes in failing to recognise the potential threats. Accountability of information also becomes less accurate when non-authorised users can access and manipulate data although they do not have the privileges to execute such activities [71]. It is, therefore, the solution that proposes the need to address global security needs that cover all or most of the scenarios in a shared networking environment.

Several solutions have been proposed to address security and access control concerns associated with the EHR systems [219, 220, 221]. In providing adequate security for the system, most of the proposed approaches discuss access control for the system. However, in the access control approaches, most of the methods use Role-Based Access Control (RBAC) to address the issues in setting up an organisational security control requirements and allocating access to different health care providers in the health care organisation. To allocate the right access to the right user, the system administrator who assigns the access controls needs a better knowledge of the internal clinical information flow, the structure of the organisation and the employees' structural relationships. Hence, the proposed solutions could not resolve the access control issues within the health care organisation settings as none of these methods considered the organisational structure and the complexity of a dynamic environment where the EHR system is used. Similarly, several Purpose-Based Access Control (PBAC) models have also been proposed recently to secure sensitive data in health care [222, 223]. In this approach, access is granted when the purpose of the entry to access a piece of particular information is met and satisfied with the given criteria. However, as health care is such a multifaceted domain incorporating numerous stakeholders with diverse-range of responsibilities and purposes, a PBAC solution alone cannot satisfy all the stakeholders' privacy protection needs.

The EHR systems including MyHR include a large amount of sensitive data from thousands of health care provider organisations nation-wide and therefore the system is open to misuses and threats more likely than an in-house clinical system of a health care organisation. It is also pointed out that large amounts of sensitive health care information held in data centres are vulnerable to lose, leakage, or theft [280]. For this reason, in recent times, personal sensitive health information of hundreds of thousands of patients has been stolen because of the security gaps in hospitals, insurance companies, and some government agencies [281]. The health data is vulnerable to abuse by those looking to get profit from it. For example, some medical companies are interested in buying information about doctors' prescribing habits to improve their businesses [282]. The World Privacy Forum (WPF) also advises that the sensitive health electronic information, especially when stored by a third party, is susceptible to blind subpoena or change in user agreements. Especially, businesses such as hospitals and law firms, which are required by law to respect users' privacy, may be at risk of a lawsuit simply for using a Cloud computing service, even if the information is not leaked [283]. Additionally, in contrast, some businesses disagree with the options in setting up proper security controls to the patient's sensitive health information to protect them because of their business interest and the profit are conflicting the idea. Moreover, in a shared networked environment, concerns on privacy, security, and confidentiality are extreme. Mobile accessibility makes this concern even worse. The wireless networks also can be used to boost the accessibility of the EHR system. This allows a user to access the network from outside a health care organisation. However, the users can request access from more than one location where a diverse level of access control and/or security controls in place. The user privilege and admin domain control are varied from one location to another. For example, a nurse cannot change a medication while a doctor does it. Therefore, *Mavridis and al.* [298] argue that it is important in a distributed medical information system to be able to determine the location in which the access request is made.

In the implementation of an EHR, all the concerns and challenges are not related to just about the privacy and security of the system. There is a wide range of challenges to face and overcome to make the use of the system. For example, the MyHR implementation process in Australia faces a broad range of other issues than privacy and security. First of all, the patients and health care providers and their organisations must register with the department of health to join the system. With the recent opt-out concept, the patients do not need to register themselves; however, the registration process remains for health care

providers and their organisations. The registration process involves too much paperwork and follow-ups and they are also time-demanding.

The other issue is compatibility. For a health care provider to access the MyHR system, either they should have a compatible clinical software system that complies with the MyHR or via web-based portal using their individual NASH PKI certificate that they received after they registered with the department. Using the individual NASH certificate, the providers can only view the details that uploaded for their patients and they cannot upload a copy of the present consultation details or update the current clinical conditions and medications. This inability pushes the health care providers to mainly rely on their organisations' clinical system. However, the incompatibility of the organisations' clinical system restricts the usage of the system. Although the majority of the general practice clinical software programs are compatible with the MyHR system, the majority of the other health care provider groups such as allied health, medical specialists, and hospital software systems are still not compatible. For this reason, overall, most of the organisations are not in a position to use the system even if they have registered with the system and received all the credentials and digital certificates. The software vendors are not yet completely convinced of the adoption of the system. The practical difficulties, unclear requirements and specifications, additional development cost, and training and education needs are some of the obvious concerns that the software vendors face in making their software systems compatible with the MyHRs.

The PKI certificates necessity creates some additional problems with the MyHR system continuation and maintenance. Two PKI certificates must be deployed to access the MyHR through an organisation clinical system – the NASH and the Site. While these certificates create some technical issues where the provider organisations require further supports from IT providers, Medicare technical teams, software vendors or Primary Health Network (PHN) personnel, they expire on a regular-basis and need attention in updating them to continue to work with the MyHR system. The NASH certificate expires every two years and the Site one expires every four years. In most cases, the health care provider organisation are not aware when one of this certificate expires, how to get a new one and from where they get it. For example, every certificate comes from different departments to perform a different function. Every certificate has an identification passcode the same as a password. The organisations used to receive them by post on different days, for example,

for security purposes, the NASH certificate arrives one day on a CD and its passcode comes another day. The department has now changed the way they issue the certificates. For NASH certificate, the health care provider organisation should request online through Provider Digital Access (PRODA) portal. Once the request was successful, in a few minutes, the NASH certificate can be downloaded and the passcode is sent by SMS to the practice manager who registered with the system as responsible. Furthermore, creating a PRODA account does not appear as an easy task. A significant amount of provider organisations do have issues in creating and using PRODA online services. On the other hand, for the Site certificate, the Medicare updates every four years via online to the billing system that does the Medicare online claiming for the health care provider organisations automatically. Medicare currently no longer sends the Site PKI certificate by post. However, this automatic update method does not apply for a clinical system of the organisation to work with the MyHR system. To update the clinical system, the updated certificate from the billing system needs to be exported from the server of the billing system using the PKI manager export options. To perform this task, the organisation requires another password that would have been used a long while ago with the server settings named *store password*. This task is more technical for the ordinary health care provider organisation's staff and thus, they may need technical assistance from the IT providers, software vendors or PHN technical support team.

Generally, the health care provider organisations do have high-level security in place for their IT infrastructure and this is one of the accreditation requirements by the RACGP. One of the key high-level security controls is suitable anti-virus protection for the computers and servers. In some cases, this basic protection control disables and blocks the connections and communications between the organisations' servers and the MyHR server. A poor and slow Internet connection also, eventually, impacts the MyHR access or unavailability of the system. Even though the Government has expected that the National Broad Band (NBN) high-speed Internet scheme will solve the issues with the MyHR faster access, the NBN deployment faces its issues and the plan has, still, not yet met its target and the objective.

The training and education on the MyHR initiative are also lacking. In some cases, although the provider organisations have registered and the MyHR is connected to their local clinical systems, the individual providers do not know how to use the MyHR including uploading

SHS and ES health summaries to the MyHR and viewing the uploaded documents using their clinical systems. Also, the inadequate training or education on the system consequences a lack of understanding or knowledge about the system and this eventually leads to a misconception of the whole idea of the system. For instance, many health care providers assume that patients have the ability to amend the medication or medical conditions that they already uploaded. These kinds of assumptions, ultimately, impact the implementation of the system negatively. Another example is that the health care providers have a misunderstanding that the process of creating and uploading an SHS or an ES to the MyHR is a great deal of time. In reality, the time that a health care provider spends on his or her usual patient is not long. The health care providers do not conscious until they practice it. However, having mentioned that, the information the providers share through MyHR should be precise and up-to-date to receive the whole purpose of the system. The inaccuracy and outdated health information would not only be worthless at the point of care but also put the patient health care outcome at risk. Hence, the health care providers must review the health information of a patient before uploading them to ensure the information that they share is useful and meaningful for future care. In this perspective, the providers using an international standard medical terminology is paramount. However, they often use plain text for medication and/ or medical conditions to record the patients' health information. This circumstance leads to incorrect spellings and ultimately results in an unidentified medication and/ or medical condition. Therefore, it is important to use predefined medical terminology and coding that accept international standards from a dropdown list rather than a plain text option.

Moreover, every clinical system uses different procedures to access the MyHR whether it is an upload or a view. This inconsistency of the clinical software application also makes the use of the system difficult. For example, when a health care provider practices in two different organisations where the clinical systems are varied cannot follow the same method to upload or view the record. Therefore, there should be the reliability of the process of using any clinical systems.

2.5 Access Control

In addition to Section 1.1.6 that discusses the background and importance of access control in the EHR systems, this section analyses the related work.

The researchers have developed different access control methods to access a resource in computing systems [213] including in health care settings. Most of these methods discuss a list of authorisations to an entity in an access control settings that describes the user rights of every substance with relevance to each entity. These methods are not appropriate for larger health care organisations where several substances and entities involved. *Khayat and Abdallah* [262] proposed a proper model for flat role-based access control that overcomes some of the identified problems in access control as it utilises the flat approach. This model focuses only on the users' roles and it does not contemplate the problem-oriented method in health care settings, for example, creating a group of patients based on the medical condition such as mental health or diabetes. *Choudhri et al.* [263] presented a model that uses mobile technology in health care access settings. This is a dynamic reliance model where a usual health care provider of a patient can give access to another provider in the same user domain control. Access to the new provider can be either full or limited. In most cases, the patients are not aware of the delegations. This raises further privacy concerns and questions. Also, *Evered and Bogeholz* [259] completed a case study that proposed the access control requirements for a health information system. The study used a fixed access control list and it discovered that a technique is insufficient to provide the required protection while the policy restrictions are in place.

The privacy, confidentiality and security concerns in health care settings, ultimately, refer to access control. The term access control is simply defined as *the ability to permit or deny the use of something by someone* [5]. The main purpose of an access control mechanism is to preserve data privacy through authorising a permitted user to access a required dataset [6]. There are different types of access control mechanisms existing for this purpose. The main access control principles are (i) Discretionary Access Control, (ii) Mandatory Access Control, (iii) Role-Based Access Control, (iv) Purpose-Based Access Control (PBAC) and (v) Attribute-Based Access Control (ABAC) [7].

2.5.1 Discretionary Access Control

Discretionary Access Control (DAC) is an access control constraint established by the owner or system administrator to restrict access to an object. This model considered as a weakened approach for a shared environment based on its level of security options. Also, once a user is set to access an object by the owner, then the user can pass the user's rights

to another user without the owner's involvement [8]. This risk circumstances read access transitive and the policies are open for Trojan Horse Attack [9].

2.5.2 Mandatory Access Control

In Mandatory Access Control (MAC), a central authority controls what information is to be accessible by whom [10]. However, security labelling in MAC is not flexible and is not convenient for task execution [214]. The central authority control of the MAC is built by privacy and security policies of a set of security and privacy policies inhibited consistent with activates such as user grouping, structure, and verification. Compared to the DAC model, MAC setting can provide more security controls including preventing trojan horse attacks. Therefore, the integrity of the data objects can be protected by using the *Read Up* and *Write Down* Rules. However, with the MAC model, the individual owner of an object has no right to control the access. This inflexible option in a dynamic environment like health care does not suit the nature of the settings and the requirements of the patients' EHRs [11].

2.5.3 Role-Based Access Control

In Role-Based Access Control (RBAC), the access rights are linked with roles, and users are assigned to appropriate roles [9, 215]. This model has been considered in health systems [216] as the role hierarchy permits the senior role to inherit from junior roles. *Reid et al.* [260] examined the RBAC model as a suitable method for access control in health care settings. In this proposal, the access control is considered as a patient-centred role known as a *care team* and a group access policy applied for a sub-group object in a health care organisation. However, it is discovered that the variety of access policy provided by the RBAC is not sufficient to protect the sensitive health information in the sector. Subsequently, *Motta and Furuie* [261] extended the RBAC reference model by introducing contextual authorisation. The authorisation element not only applies the authorisation whether the access granted or denied, but also it should consider other related factors including user relationships, time and location of access, and patient circumstances. The RBAC policy practices the need-to-know attitude to allocate permissions for users' roles. Given the fact that the health care providers require timely access to the health information to enable better patient care, the RBAC modules permit some health care providers to get additional access rights than others. This supplementary mechanism is more convenient and needed in health care settings. That is why the RBAC models have attracted significant

research interest in the last decade [224, 225, 294, 295], and have been widely used to protect privacy in health care systems [226, 227, 228].

However, using this supplementary mechanism to misuse or overuse may create a negative response for the model. For example, recently, an extensive study of audit logs from a hospital EHR system in Norway [229] found that those exceptional mechanisms have been significantly overused. Moreover, *Cederquist et al*. proposed the a-posteriori access control framework, called audit-based compliance control [230], and illustrated its application in the EHR setting [231]. In this method, there is no constraint applied to the health care providers during the consultation process, however, later the health care providers need to provide justification and relevancy to why and under what circumstances they accessed a specific piece of information according to the associated policy. Even though this method offers excessive flexibility for health care providers during the consultation and health care delivery, it fails to prevent the users those that cannot be held responsible to access the health records. Consequently, this proves a need for an innovative access control model that offers a better balance between preserving privacy (and security) and the flexibility in the use of EHR systems.

The RBAC model also needs simpler administration requirements as the system administrator requires only revoking and assigning the new suitable members in an organisation according to their job function. Also, the RBAC is known to be policy-neutral [296, 297] and supports security policy objectives as least privilege and static and dynamic separation of duty constraints [295]. Moreover, the RBAC shows that it can be set up to implement mandatory and discretionary access control policies and recent models [296 [297], extend the RBAC model by defining progressive restrictions on each role that is associated with every user. However, the RBAC does not incorporate with other access parameters or related data that are significant in permitting access to the users [12]. Additionally, in presenting a passive access control model, the RBAC has failed to capture the dynamic accountabilities of users in provision of their workflows that require active motivation of access rights to perform some specific tasks, for example, in a solo health care provider organisation setting, a reception staff may require permission to access a follow up on some medical conditions like screening.

2.5.4 Purpose Based Access Control

Purpose Based Access Control (PBAC) is based on the concept of involving data entities with purposes [13]. Many researchers have identified that better privacy preservation can be promised by allocating entities with purposes [14]. In most cases, RBAC and PBAC become similar to purposes depend on the requirements of their roles. However, *Al-Fedaghi* [15] describes that the PBAC leads to a great deal of complexity at the access control level. Especially in a health care environment that identified as one of the dynamic and complex settings, considering all users' needs with purposes and assigning user rights and privileges according to that needs becomes a difficult task. For this reason, using just the PBAC model to cover all users' circumstances is challenging and shows more complexity in the administration pace of the model.

2.5.5 Attribute-Based Access Control

Attribute-Based Access Control (ABAC) is also known as policy-based access control. This model describes an access control prototype that access privileges are allowed for users over the use of policies that linked to attributes. The policies can be used any type of attributes such as user, resource, environment, and entity. The ABAC offers an improved access control mechanism that includes dynamic, context-aware and risk intelligence capabilities. Therefore, this model supports to achieve a competent monitoring facility, active Cloud amenities, reduced time-to-market with new clinical software applications, and a top-down attitude for controlling through clear policy implementation. In the ABAC concept, attributes are used as building blocks along with structured language that describes various access control rules and defines user access requests. The attributes include labels or properties that are used to define all the objects that must be reflected in the authorisation process. Each attribute consists of a key-value pair such as *Role=Manager* [326]. Therefore, the ABAC can offer an improved and appropriate access control method that permits several various inputs into the permission of the access control. Several potential combinations of the variables are used to represent a larger and more conclusive set of potential rules, policies, or constraints for the access. *Tyson Macaulay*, in *RiOT* control [327], points out that ABAC empowers systems administrators to apply access control policy without a thorough previous understanding of the particular subject. The access control policies that can be used in ABAC are only restricted to the computational

programming language and the fertility of the available attributes. For this reason, ABAC cannot be applied in every aspects and circumstance of a health care provider organisation.

2.6 Access Control of the MyHR system

Similar to other EHR systems, access control mechanisms offer the essential security services of identification, authentication, authorisation, and accountability to enter into the MyHR system. An access control mechanism provides different levels of security options. While the identification and authentication services determine who can log into a system including MyHRs, the authorisation controls different privileges or user rights for the system (typically categorised into three levels: full access, limited access, and basic access) in accordance with an employee's role in a health care organisation and the accountability identifies the subject a user accessed during his or her access duration. For example, accountability offers the audit-log details for the MyHR system.

The staff members that have the duties in their role only should access the MyHR system in a health care provider setting. When a provider organisation registers for the system, two responsible roles are created such as Responsible Officer (RO) and Organisation Maintenance Officer (OMO). While the RO is responsible for higher-level of legal obligations, the OMO has some operational accountability towards maintaining the system. However, both the RO and OMO can assign the users who can access the MyHRs and will be responsible for other related activities including staff leaving and joining the organisation, any security issues that compromise user accounts, and any changes of duties that require on cancel access to the MyHR system. In the meantime, the OMO administers the operational activities such as ensuring digital certificates are up-to-date, preserving privacy and security, and essential security controls and access controls are in place.

The authorised health care providers who are involved in a patient's care can only access the patient's MyHR. However, within a health care organisation, with the current access control, any health care provider can access a patient's MyHR. The current access control mechanisms in place with the clinical system and MyHR are unable to prevent the health information from other than the usual health care provider within an organisation. Accessing a patient's health record by a health care provider who is not involved in the patient's care does not always detect as a data breach or unauthorised access, because there

are instances where a usual health care provider of a patient seeks a second opinion from his or her colleague within an organisation. Also, a health care provider who is under a senior provider's supervision often discusses medical conditions with the senior provider. In these circumstances, sharing the information with other health care providers becomes necessary. However, on the other hand, there are situations where the patients may not want to share their sensitive information with other health care providers than the usual provider. Obtaining consent from the patient can resolve this precarious circumstance. To make this circumstance even worse, non-clinical staff including admin or receptionist can access clinically related information including the MyHR to target patients to improve the business of the organisation. For example, the practice needs to follow up for health assessment checks due and send reminders to the mainstream patients or identified chronic disease high-risk patients to recall for further test [131 - Author's previous publication]. These access over-rights circumstances, eventually, lead to abuse of sensitive health information and contribute to the increased concern of privacy and confidentiality [13]. Furthermore, the system operator of the MyHR who administrates the system may intentionally leak patients' clinical information. The current settings of the access control mechanisms do not prevent this kind of breach [354 - Author's previous publication].

The audit trail facility of the MyHR captures all-access histories of the record. The access history information that a patient can view includes the name of the health care provider organisation that accessed the health record, the role of the person who accessed and the nature of the access. However, the actual name of the provider or person who accessed the record is not available. In a larger health care organisation with numerous providers working, it is difficult to find out which provider has accessed. Also, many argue that once the damaged happened after accessing the sensitive information, the damage will be either a privacy breach or data theft, it is too late to aware to prevent sensitive health information. Figure 3 shows the access history of the MyHR that the patients can view.

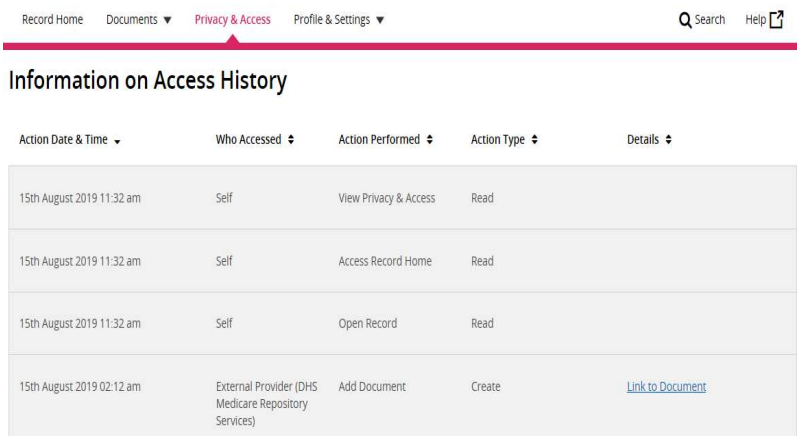


Figure 3: The MyHR access history audit trail

A patient or consumer can link and access the MyHR through their myGov account where other online government services are connected such as the Medicare, Centrelink and Australian Taxation Office (ATO). Although it is convenient for patients as it reduces one more password to remember, in contrast, having all government online services in one place increases the risk of someone stealing the credentials. Moreover, the MyHR has some access control mechanisms where the patients can go to their record and enable the settings to manage the privacy and confidentiality of the record. The settings include;

(i) Creating code and providing to those health care providers need access to their records. In other words, without the code of any health care provider, even the usual provider cannot access the patient health record. The option of managing access for health care provider organisation by a patient is exposed in figure 4.

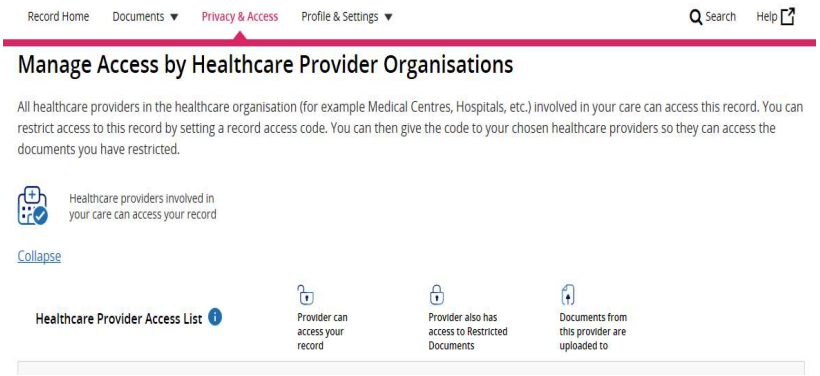


Figure 4: The MyHR access control restrictions by health care provider organisations

(ii) Assigning an authorised representative, for example, children or elders who cannot access online can involve on behalf of the patient.

(iii) Setting an automatic notification option. This will keep the patient informed via SMS or email who access records when.

(iv) Enabling the settings to access the documents such as SHSs, personal health summaries and advance care plan. The options provide patients to restrict hide or remove the specific documents from the system. In the case of hiding, the document needs to be reinstated to view it, however, once it is removed by the patient, the document cannot access completely in any circumstances including emergency access. Figure 5 displays the MyHR settings for restrict, hide or remove documents from the record.

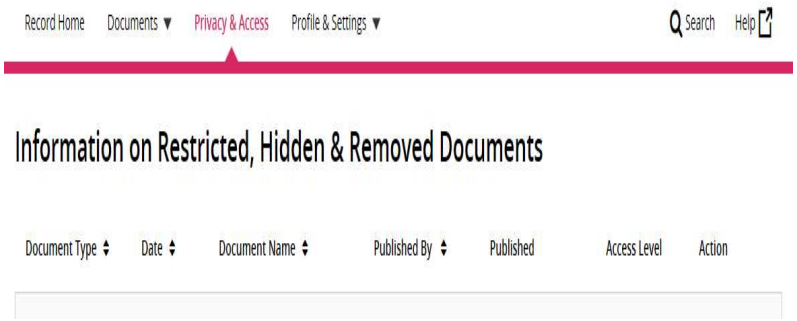


Figure 5: The MyHR access control restrictions by documents

Even though these controls provide more security options in preserving the privacy of the health information over the MyHR system, the default setting has no controls until the patient logon the system and creates theses controls. The majority of the population, who have got a MyHR, especially through the opt-out method, are not aware that there is such control mechanism existing for them.

Under an emergency like a serious risk to patient health or life, a registered health care provider can access the patient's MyHR by providing the patient's details such as surname, Medicare number, date of birth and gender to gain the access. The access can be made either through the health care provider organisation's compatible clinical system or via the web-based MyHR portal. The emergency access supersedes the current access control settings and can last for a maximum of five days. In reality, the necessity of emergency access is proved, however, defining the verification phase of the emergency access to

whether the access is needed or not is tough. The patient also nominates a family member, friend or carer as his or her representative to act by the patient's will and preferences. This access may be full, restricted or basic levels to access all documents. Although many of these access levels cannot cancel the MyHR, they lead to misuse of the health information as another person cannot represent all aspects of the patient.

2.7 Health care database attack analysis

In addition to access control mechanisms, it is also important to identify the spectrum of attacks or misuse that has been conducted by attackers in the past. A wide range of attacks has been documented. Therefore, it is essential to know the different potential cyber-attacks and security breaches that happened in health care based databases, to design an appropriate health data security system. To achieve this goal, the literature review has been performed to discuss the EHR related security breaches and various major data attacks. *Amichai Schulman and Imperva* [16] describe that the enterprise database infrastructures, which often contain the crown jewels of an organisation, are subject to a wide range of attacks. Hence, the health care sector and sensitive health information are more vulnerable to the cyber-attacks. For example, one of the major health database attacks was that hackers have stolen more than 1.5 million Singaporeans' health records in 2018.

2.7.1 EHR related security breaches

Issues of confidentiality and abuse of data cause many health care providers to oppose the coordination of medical databases despite their potential benefits [72]. The followings are some of the incidents of security breaches about EHRs:

- Researchers from the University of Minnesota mistakenly revealed the names of deceased kidney donors to the recipients in a survey [73, 74, 75].
- A hacker had access to sensitive health data from an unidentified medical centre in New York and another in Holland [76, 77].
- A hacker infiltrated the University of Washington's Medical Centre computer system and stole at least 5000 cardiology and rehabilitation patients' records [328].

- A Florida state public health worker brought home a computer disk with the names of 4000 HIV positive patients and shared the contents with two Florida newspapers [78, 79 - Author's previous publication]

2.7.2 Categories of health data attacks

A review of previous attacks has revealed the following main methods utilised to obtain sensitive health information [78 - Author's previous publication].

1. An excessive privilege granted to staff
2. Privilege abuse
3. Unauthorised privilege elevation
4. Platform vulnerabilities
5. SQL injection
6. Weak audit
7. Weak authentication
8. Exposure of back-up data

A better understanding of the past health data cyberattack and the methods will assist in designing an appropriate security model in the health sector. The main database cyberattacks that have been observed in the past are discussed in table 6 [79 - Author's previous publication].

Table 6: Potential database attacks in the health care environment

	Categories of attack	Description	Example
1	Excessive privileges	Application users are granted exceed privileges than the requirements of their job functions	An employee whose job requires the name and address of other employees takes privileges to view the salary information as well.
2	Privilege abuse	Application users may abuse legitimate data access privileges for unauthorised purposes	A user with privileges to view employee details may abuse that privileges to retrieve all employee records.
3	Unauthorised privilege elevation	Attackers may take advantage of vulnerabilities in DBMS software to convert low-level access	Sometimes, an attacker may take advantage of database buffer

		privileges to high-level access privileges	overflow vulnerability to grant administrative privileges.
4	Platform vulnerabilities	Sometimes the attackers take advantage of the vulnerabilities in underlying operating systems may lead to unauthorised data access or corruption	"The blaster worm took advantage of a Windows 2000 vulnerability to take down target servers"[05]
5	SQL injection	Users may take advantage of vulnerabilities in front-end web applications and stored procedures to send unauthorised database queries.	Users may take advantage of vulnerabilities in front-end web applications and stored procedures to send unauthorised database queries.
6	Weak audit	Weak audit policy and technology represent risks in terms of compliance, deterrence, detection, forensics, and recovery [05]. The Database Management System (DBMS) software provides weak audit solutions.	DBMS products very rarely log the detail about what application was used, the source IP address and what queries was fail
7	Weak authentication	Sometimes weak authentication allows attackers to assume the identity of legitimate database users.	Most of the time, the users use their name, personal identification, meaningful words, a plain text as a password.
8	Exposure of back-up data	Sometimes attacks have involved the theft of database backup tapes and hard disks	Attackers feel free in attacking backup from easy destination rather than attack the databases directly itself

2.8 Towards potential solutions

Taking every aspect into account, based on the above discussion and analysis and moving towards an appropriate solution to overcome (i) insiders' unauthorised access, (ii) availability of de-identified data sets for other purposes like research and (iii) ensuring high

level of security for the sensitive health data that is stored in the Cloud, a three tier security model is proposed.

(i) Tier one – an improved access control mechanism
(ii) Tier two – an intermediate state of database access or insensitive data view
(iii) Tier three – cryptography or data encryption and decryption technique

2.8.1 Improved Access Control

In the traditional health care settings, the users' levels and authorisations are allocated according to the accountabilities provided within the organisation. This arrangement assists the users to perform certain given tasks by their position description. Also, the health care settings cover several different participants involved in various positions. The patients are central to the health care delivery and in the environment they have direct interactions with many of these participants or stakeholders such as a usual doctor, nurses, specialist doctor, admin staff, and receptionists. Every stakeholder has his or her job role and tasks that need to interact with the patient to perform the specific task. The specific piece of the task may involve a different type of information and use a different software application. For example, while a receptionist books a time for a consultation using an appointment software application, a nurse enters progress notes for the visit using the clinical application that the usual doctor can access. Regarding access control, the location of the user is also one of the considerable factors. The job role can be completed from many predefined locations and the role's accountability can also be varied depending on the location. For instance, while a health care provider accesses a patient's MyHR in his or her provider organisation through a compatible clinical application, the provider also can access the record via a wireless connection from a hospital emergency department. In this case, the access locations are varied. Therefore, the potential location of the access also needs to be considered when proposing a suitable security method to preserve the privacy and security of sensitive health information.

With the increased use of mobile devices and the evidence of the benefits in health care settings, the identification of location becomes essential to ensure the privacy and security of the health information. When a health care provider accesses the MyHR system from a location using a mobile device, the system should be able to identify the location of the mobile terminal where the access was requested. This location of the request must also be influenced by the authorisation decision making. This is most essential in health care

settings because unauthorised access to health information may have severe consequences. In a wired structure, on the other hand, this task can be effortlessly achieved based on the physical/ logical addresses of the hardware equipment connected. It means that access to a specific sensitive service is based on the physical/ logical address of a workstation. However, this will not be possible with a wireless network because of the distance of the signal reception area of the wireless service points. Furthermore, obtaining the physical address of the access becomes impractical while a mobile device is moving. Therefore, the health care provider organisation's privacy policy and procedure must clarify and discuss the facts associated with wireless use [299].

The security policy for an organisation must also describe the various roles of the organisation and the authorisation process with the specific separate locations in addition to the levels of user rights. The framework also has to contain the notion of hierarchies that are natural means for structuring roles to reflect the organisation's lines of authority and responsibility [295]. Hence, each level of the user privileges must reflect the role of a specific staff member's responsibility in a health care organisation.

2.8.2 Pseudonymisation

In health care settings, as discussed previously, a wide range of users use the system for various purposes. In some cases, non-clinical staff members of the organisation require clinically related information and there are other instances where researches or research institutes may need access to the health information in the EHRs. The information given as it is with identification links will lead to high-risk of misuses and/ or privacy breaches. Therefore, the sensitive data should be de-identified before hand-over to the staff that has no right to access or to third-parties outside the organisation. In other words, while the sensitive health data is being de-identified and protected, the other parts of the relevant information and de-identified datasets must be provided without the risk of privacy. To achieve this objective, *pseudonymisation* technique is used to protect the system while it is shared with the users who require the data to satisfy their job functions. *Pseudonymisation* is a data management and de-identification process that replaces the personally identifiable (sensitive) information fields within a data record by one or more synthetic identifiers or pseudonyms. In this process, a single pseudonym for each replaced field or collection of replaced fields creates the data record less identifiable while remaining appropriate for data analysis, research, and data processing purposes. The pseudonymity is an approach that

offers a method of visible privacy and entails legal, organisational or technical procedures; consequently, the relationship between fields can only be achieved under described and precise conditions. A pseudonymous record or transaction is one that cannot – in the ordinary course of events – be associated with a particular individual [249, 251]. Even though the existing approaches for *pseudonymisation* have some drawbacks that pose a threat to the privacy and confidentiality of stored patients' data [248, 250, 252], others have not yet been entirely realised in the field of patient-related privacy issues [2, 5, 6, 7].

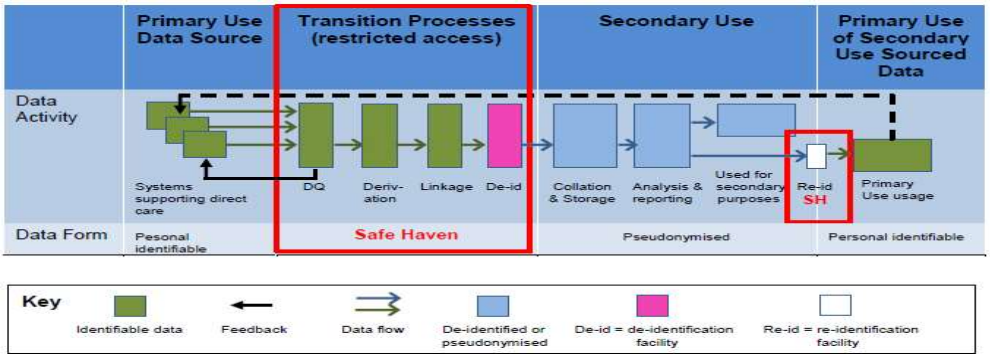


Figure 6: Pseudonymisation process

Figure 6 above illustrates the *pseudonymisation* process with four stages. The primary use data source is complete data that includes all data fields as it is. In the second stage, the data transition happens and the output will be the *pseudnymised* data which is de-identified in the third stage. In the fourth stage, again the data will be re-identified for the primary use with full access. Therefore, in the process, non-clinical staff and researchers can access the third stage which is *pseudonymised* data.

2.8.3 Cryptography technique

Several new cryptographic schemes have been proposed to secure and preserve the privacy of EHRs [275, 276, 277, 278]. The Patient Controlled Encryption (PCE) [9] design proposes a hierarchical-based encryption scheme for protecting EHRs that does not rely on a trusted online server to intermediate access control decisions. Although the scheme permits patients to get access to their health records and empower remote searches on the encrypted records, the classification of the model is inefficiency in practical. For example, a separate decryption key is necessary to share the information in a health record with different levels of sensitivity categories that the system classified. This inefficiency

displays a natural constraint for the classification encryption model that prevents flexible access arrangements.

Although an Attribute-Based Encryption (ABE) method preserves an encrypted access control that similar to the PCE model, it supports for further meaningful access level settings. *Ibraimi et al.* [276] proposed a multi-authority CP-ABE (Cipher Text Attribute-Based Encryption) protocol for securing EHRs through diverse domains such as health care providers, close friends, and immediate family members. *Ibraimi et al.* [277] also proposed a simplified CP-ABE system for EHRs to resolve the cancelation of user attributes before an expiration date. However, this model depends on a facilitator that preserves an attribute cancelation list. The mediator only offers tokens for decryption that related to a ciphertext when the user's attributes have not been cancelled. Narayan et al. [278] suggested an EHR system that uses an optional transmission CP-ABE model that shared with Public Key Encryption with Keyword Search (PEKS) methods to protect and permit a reserved search of health records. This model offers the method of straight cancelation of user access without re-encrypting the data by using the broadcast encryption process. The keyword searchability enables users to execute keyword matching without prior knowledge of the equivalent plaintext. The weakness of the ABE techniques is that they are mostly considered for online EHR systems only. Additionally, these previous works [275, 276, 277, 278] do not consider implementation challenges with their proposed schemes. Also, they do not discuss concerns include ciphertext overhead on the records, cryptographic efficiency, and policy administration that may occur while implementing such systems.

However, all in all, the cryptographic method is considered one of the suitable techniques to maintain the privacy, confidentiality and the security of the health information systems in a shared environment. To exchange the data safely in the Cloud concept, cryptographic solutions are appropriate by using the public key arrangement [318]. However, before storing sensitive information such as a health record in the Cloud, the information must be encrypted. In practice, this is not an easy task as, in most cases, the system administrators have to perform this task and the user has to rely on them to complete it. This dependency circumstances also increase the risk of privacy and misuse. Providentially, these circumstances are now removed with several new cryptographic techniques and the full right of the information is given to its user or owner of the origin.

However, these circumstances are varied with an EHR system as the owner of the information is a patient. To manage this prospective risk of such privacy concerns, many EHRs systems now allow the patients to encrypt their health records before storing it in the Cloud [319, 320, 321]. *Van der Haak et al.* [322] proposed another model that uses digital signatures and public-key validation to meet the legal prerequisites for cross-institutional transfer of EHRs. In another concept, *Ateniese, Curtmola, de Medeiros & Davis* [323] used the pseudonyms technique to maintain patients' privacy. *Layouni, Verslype, Sandikkaya, De Decker & Vangheluwe* [324] developed monitoring equipment that exchanges messages between a patient from home and a health care provider from the organisation.

Even though the proposed methods provide more security and maintain the privacy for sensitive health information, the information must be downloaded from the Cloud to alter or update an element of the record. This inefficient constraint destructs the whole purpose of the EHR systems using the Cloud concept. Consequently, using these proposed methods in the deployment of the MyHR is unusable. However, cryptographic solutions with encryption and decryption based techniques are exceptionally essential in ensuring the privacy and security of sensitive health data.

Chapter 3

Research Design and Methodology

In this chapter, the methodological approach and research stages are introduced and described in detail. The research is undertaken considering an analytic generalisation of the literature review study. A porotype implementation followed by a test and simulation is conducted to analyse and evaluate the proposed solution.

3.1 Research Design

The exploratory research has been based on the analytic generalisation of the literature review study. In addition to the analysis of the literature review study, the research is focused on modelling of a software specification and the controlled simulation and test of a security model. The security mechanism is designed to secure patients' sensitive health information in the Cloud including EHRs.

3.2 Research Methodology

This research is based on the analysis of the literature review study and the development of software components as a method of study. The development of a prototype software interface will facilitate the analysis of security measures for data stored in the EHRs in a shared care environment. Therefore, the assumptions obtained would be based on an analytical generalisation of the data collected in the literature review through the different stages of this research.

The prototype development is a useful method to study effective design, delivery, use and impact of information technology [91] and system development approach is considered an applied research method which is used to test the validity and limitations of a proposed theory [92]. In this view, the system development method allows both the implementation of the application used to illustrate theory and the refinement of the proposed theory based on the data obtained from observations made during its implementation and testing [92,

93]. Therefore, system development could be a central component of a multi-methodological research cycle [94]. To conduct software analysis, a prototype version of the proposed architecture would be implemented. The prototype will be configured as a set of integrated libraries and components based on a conceptual approach for secure storage of EHRs as described in Chapter 6.

3.3 Research Stages

The research has been undertaken into three stages and two supporting areas of methods. The literature review has the purpose of analysing state of art regarding the security mechanisms and approaches used to protect the access of EHRs with a special interest in the protection of patients' confidentiality. The conceptual approach discusses the need for the new model to protect the EHR systems that grow rapidly with the advancement of the Cloud computing concept.

The literature review and the conceptual approach go through the following major research areas that preserve health data privacy and security in the EHRs.

(1) Access Control

(2) An intermediate State of Database / Psuedonymisation

(3) Cryptography / data encryption and decryption technique

3.3.1 Access Control

Shon Harris defines that access control is the ability to permit or deny the use of something by someone at the Certified Information Systems Security Professional (CISSP) exam guide [95]. In the computer information security domain, access control offers fundamental substance protection of the system that covers a wide range of aspects include biometric scans, digital certificates, and even mechanical systems in addition to the processes of authentication, authorisation, and audit. Also, the term access control not only means using a user ID and password for an operating system or platform but also it is applicable for several different individual software applications. Additionally, the electronic access control becomes more common indoor entry phones, many with visual verification by small video cameras, or swipe cards or tags that are read by computer-operated detectors, are all readily available [96].

Taking the importance of access control into account, the method cannot be evaded for a system like EHR including the MyHR. However, based on the literature review on this

domain in Section 2.5, an improved version of this technique is essential in preserving the privacy and providing security of the sensitive information systems like the MyHR.

3.3.2 An Intermediate State of Database (ISD)/ Pseudonymisation

Employees of an organisation access databases for different purposes. In most cases, they access for analysing trends, identifying accounts, processing documents, etc. These purposes can be achieved with the de-sensitive information available in the databases. If it is possible to access the part of the databases where de-sensitive information available to employees of an organisation then the sensitive information can be protected and prevented from internal abuse. In this respect and based on the literature review, a *pseudonymisation* technique is identified as suitable. The *Sapior Company* developed this concept to protect patients' records for NHS. The *Sapior Company* [97] addressed that adopting a pseudonym can preserve privacy. Sensitive data can be protected at the same time as allowing users access to less critical elements using a technique called *pseudonymisation*.

The key benefit of the *pseudonymisation* method is that while it is preserving the privacy of the sensitive information by hiding the sensitive information from the view, the technique is still offering data relationships for searches without capturing all the values of the data outside the exact context of the interaction and the original data cannot be amended from an unauthorised access.

3.3.3 Cryptography / data encryption technique

Rutgers University (RU) evaluation security processes describe [98] that the term briefly as data encryption is a means of scrambling the data so that it can only be read by the person(s) holding the 'key' - a password of some sort. Without the 'key', the cipher cannot be broken and the data remains secure. Using the key, the cipher is decrypted and the data is returned to its original value or state.

Variety of algorithm exists to perform the data encryption/cryptography. The research undertaken involves assessing some useful algorithms and the cryptanalysis to gain a good understanding of the area. This understanding will be helpful to achieve the aim of this project (i.e.; developing a strong algorithm). Overview of existing algorithms and the proposed algorithm are discussed in detail in Chapter 5: Description of the proposed system.

It is clear that the research undertaken will be helpful to achieve the objectives of the project. All the findings from the literature review are applied to make this proposed method successful. The specific methods that are going to be developed in the project will be discussed in detail in Chapter 4: Conceptual Approach and Analysis.

3.4 Health Database security

A database system is the most valuable asset for any organisation as they hold important data of the business or service. However, the health database becomes even more precious property for the health care organisations because of the sensitivity of the data it holds [99]. The health databases store not only health-related sensitive information that can affect the patients for lifel such as allergies, major diagnoses, major medical history, medications, and immunisations but they also include personal data of a patient such as patient name, address, phone numbers and date of birth. Therefore, preserving privacy and placing proper security controls for the health databases is paramount. The options to implement these security settings are varied. Every solution uses a different method to achieve this objective. However, understanding the process and the need in the real world scenario in health care settings would be the key to any kind of these solutions. For instance, a security white paper written by *Blake Wiedman* [100] discusses that the database security can be broken down into the key points of interest such as server security, database connections, Table Access Control (TAC) and Restricting Database Access (RDA). Furthermore, it is also revealed that the businesses and services highly depend on the security mechanisms of the data held in databases because any breaches of the security can be seriously damaging the business. That means, in today's world, the importance of database security of the information is understood. The privacy and security is, therefore, an extremely relevant subject for system developers and users of database systems.

3.5 Internal abuse in database security

The designers and developers consider outside attacks and threats at most. But the damages or attacks to databases are mostly, by internal attacks. Even though people believe that most of the data breaches and attacks are by outsiders, the researchers *Mike Chapple* and *Joaquin A. Trinanes* in [102, 103] revealed that it is a large percentage of the security breaking incidents are made by insiders, people employed within the same organisation. *Joaquin A. Trinanes* [104] also proposed that if the prior database security suggestions are followed, impairment instigated by insider's actions can be restricted and monitored. Also, the

appropriate security policies generally reduce the risks by discussing potential threats and suitable solutions for the threats. A wide range of factors including the connectivity, physical security, accessibility, and other associated matters should also be taken into account while implementing and setting up database servers. Additionally, according to *Thom Van Horn* [105] description and based on the Forrester research study [106], an information security system must address insiders' threats to provide complete protection for the databases. The Forrester study also revealed that over 70% of database attacks occurred as a consequence of insider activity. For example, database administrators know about the structure and related activities to leak sensitive information intentionally or unintentionally to unauthorised access within or outside the organisation. Therefore, a high-security method that proposes should consider and address the threats that cause by insiders.

Chapter 4

Conceptual Approach and Analysis

The conceptual approach leads the way for the methods to perform specific functions to accomplish the objective of the project, i.e. the proposed high-security system. Once the relevant research and literature reviews are performed in the identified domains within the scope, numerous questions must be answered to propose a strong security system protocol as a well-suited solution.

Based on the literature review in Section 2, the following conclusion can be made:

(i) Access control for EHRs is the basic fundamental security mechanism that provides privacy and security to the system. However, access control alone cannot offer sufficient security control for EHRs that the system requires because once someone enters into the system the data can be accessed or modified easily and there will be no further control to restrict the access. Therefore, the necessity for a combination of more than one mechanism or method is comprehended. However, an improved or advanced version of access control (with using new techniques in access control) will offer more privacy and security for the system.

(ii) Similarly, the data encryption, on the other hand, alone will not provide the complete protection for EHR systems as encrypted data is still available for data breaches. Once access control is implemented to provide the basic privacy and security requirements to the EHR system, encryption can enhance additional protection for the health databases. The data encryption techniques do not provide a different level of access privileges and cannot be used to resolve access controls related issues required in health care settings.

Moreover, on the other hand, encrypting everything completely does not make the data more secure. *Schneier Bruce*, the security guru [114] proved that a common misconception is to assume that if encrypting some data strengthens security, then encrypting everything makes all data secure. Encrypting the whole database means that all data within the

database must be decrypted to be viewed, modified or removed. *Schneier* [114] also revealed that the encryption is a performance-intensive operation thus encrypting all data will significantly affect performance. In other words, the encryption technique makes either all data unavailable or all data available (all or nothing concept). While, on one hand, access to all data creates security issues, on the other hand, the unavailability of all data fails the whole purpose of an EHR system. Also, the accessibility is harmfully affected when an encryption key is changed and the database is unreachable while the data is decrypted. To develop an appropriate security model that offers a high-level of security for health information in the EHR systems, therefore, it is obvious that both access control and data encryption must be incorporated in those proposed systems.

However, the necessity of another layer with the presence of an intermediate state of the database is recognised in addition to access control and data encryption to preserve the privacy of the EHRs. This layer offers a shorter version of the view a user requires for their role. While these de-identified and non-intelligent datasets would be beneficial for activities such as document process, targeting due and high-risk patients and further follow-ups, they also reduce the risk of privacy.

The proposed model should be implemented by (i) considering the above facts, (ii) based on the literature reviews findings, and (iii) keeping in mind that the databases and their contents are vulnerable to a host of internal and external threats, it is possible to reduce the attack vectors to near zero [115]. The following solution is proposed as the security model to preserve the privacy, to combat health database attacks and to achieve the objective and purpose of the model.

A three tiers architecture security model of the system:

(1) First Level – an improved strong access control mechanism
(2) Second Level – an intermediate state of database with de-sensitive data
(3) Third Level – cryptography (data encryption and decryption with a new strong algorithm)

In addition to the discussion and analysis in the literature review, the following components must also be analysed to develop the security model to provide a high-security mechanism for the EHRs:

- Previous health data attacks

- Assessment of the proposed model
- Current EHR architecture analysis
- Data integrity analysis
- Every level of the proposed architecture
- Existing access control
- Intermediate State of Database
- Cryptography

4.1 Previous Health Data Attack Analysis

4.1.1 Potential solutions for the categories of attacks

The health database attacks are analysed and documented in the literature review. Additionally, in this section, it is also necessary to discover the potential solutions for those different attacks documented. The following table 7 expands the potential solution for the attacks listed previously. This work is also published in one of the author's research papers [354 - Author's previous publication].

Table 7: Possible solutions for attacks in database environment

	Possible Attack	Possible Solutions	Description
1	Excessive privileges	Access Control Mechanism (ACM) and use view of the database	A proper access control mechanism restricts privileges to minimum data access for their job designation of an organisation.
2	Privileges Abuse	Access Control Policy (ACP) and use view of the database.	The Access Control Policy that not only to what data is accessible but also how data is accessed. Also, the policy must identify users who are abusing access privileges
3	Unauthorised privilege elevation	Access Control Mechanism, use view of database and Intrusion Prevention System (IPS)	Proper Control Mechanisms can detect a user who suddenly uses an unusual SQL operation. The IPS can identify a specific documented threat within the operation.
4	Platform vulnerabilities	Access control and IPS tools	It is a good way that uses IPS tools to identify and block possible attacks through database platform vulnerabilities.

5	SQL injections	Access Control Mechanism and view of the database.	A proper access control detects unauthorised queries injected via a web application or stored procedures.
6	Weak audit	Network-based audit appliances	The network-based review applications should have no influences on database performance and they function individually for users.
7	Weak authentication	Strong password and validate against the User ID	The password includes the combinations of letters, numbers, symbols, etc. User ID defined for every user.
8	Exposure of back-up data	Cryptography / Encryption	All back up should be encrypted before saving as a backup.

4.1.2 Assessment of the strengths of the solutions

As the next step, it is also necessary to weigh the strength of solutions against potential data attacks and this is assessed in table 8.

Table 8: Assessing the strengths of different solutions in providing database security

	Possible Attack	Access Control Mechanism	Views or Intermediate state of Database	Cryptography / Encryption
1	Excessive privileges	√		
2	Privileges Abuse	√		
3	Unauthorised privilege elevation	√		
4	Platform vulnerabilities	√		√
5	SQL injections	√	√	
6	Weak audit		√	
7	Weak authentication	√	√	
8	Exposure of back-up data		√	√

A layered concept with different controls techniques provides a wide range of security controls to a system like EHR. For example, considering a combined model with access control and cryptography, once a threat passed the access control layer, it cannot access intelligent meaningful data it requires as all have encrypted. Therefore, the layered solution with cryptography/ encryption can provide high-level security for sensitive data in the EHRs.

Overall, the previous data attacks can be categorised into eight major groups and this is discussed in the literature review. Further analysis and potential solutions for each of the attack groups are also described in table 7. Table 8 assesses the strengths for each data attack category in leading the way to provide high security for the databases.

4.2 Current EHR architecture analysis

A significant research study indicates that the EHR systems will be the information source for the health of populations in most of the health care environment [329] and will have a considerable effect on their health [330]. For this same reason, currently at least 23 countries all around the world are planning, designing and implementing EHRs [331]. However, establishing such systems at the national level faces several problems. Expansion and content variability of record data, difficulty in providing a specified and standard structure multiplicity, lack of common medical terminology and issues associated with privacy and security are some of them [332-335]. Discussing and providing answers to such problems is very important [336] and taking this consideration into account in the designing (architecture) of the EHR is also essential [337]. Establishing a framework for the successful implementation of electronic management in the health sector requires the architecture of the EHR [338]. The study of definitions presented on architecture in various fields like software and information system indicates that architecture is the science of study and identifying components of a phenomenon, their interrelations and also the relationship among the set of components with the environment [339, 340].

The architecture of the EHR is one of the crucial types of architecture that applied for schedule and technologies in the system [341, 342]. *Maldonado et al.* [343] described that different international bodies have worked on the definition of the architecture of the EHRs and the result of these attempts has been the establishment of such architecture standards as Clinical Document Architecture (CDA), Health Level 7 (HL7), openEHR and ISO EN 13606. Also, the HL7 type establishment of the CDA standard defines the structure and

semantics of the clinical documents [343]. The American Society for Testing and Materials (ASTM) has proposed the E1384 standard for planning the EHR especially the lifelong health record [344].

4.3 Data integrity analysis

Any security models that are developed to provide security in the health care setting must ensure health data integrity as the ultimate objective of the system. Therefore, this section analyses the data integrity of the EHR systems including the MyHR. The following data integrity framework developed by the author is also discussed in a research paper.

While much has been written about EHR related risks impacting information integrity and the subsequent actual potential impacts on quality of care and safety over at least the past decade, little has been done to systematically measure and analyse these risks, identify the root causes, and universally implement strategies (such as system design modifications and adoption of usability principles) to reduce the risks. However, attention to the potential unintended consequences of electronic documentation is growing [116, 27]. In addition to the risks to the quality and safety of patient care, apprehension about EHR related errors may be a barrier to EHR adoption and use [117].

There are also no clear standards for defining, measuring, or analysing EHR-related errors [118]. The need for identifying and analysing the EHR related risks is paramount. There will be several risks that adversely affect the EHR environment. A software flaw in an EHR system contains hundreds or thousands of medical records, such as a glitch that causes an inaccurate recording of patients' allergies or medications, which could adversely affect a large number of patients [119, 30]. These EHR system design flaws also can result from improper system use and poor system usability [120]. EHR system software vendors include copy/paste and templates functionalities in capturing documentation and these inappropriate methods lead to EHR related errors [121, 31].

Inadequate user training, human errors, disruption of system use or use of the system in ways not intended by the system developer can also result errors of the EHR system. Use of decision support systems may lead to errors of omission, whereby individuals miss important data because the system does not prompt them to notice the information, or errors of commission, whereby individuals do what the system tells or allows them to do, even when it contradicts their training and other available information [122].

The integrity of the entire EHR is reliant on the integrity of each of the following three phases shown in figure 7. The process of ensuring integrity to each phase would be different.

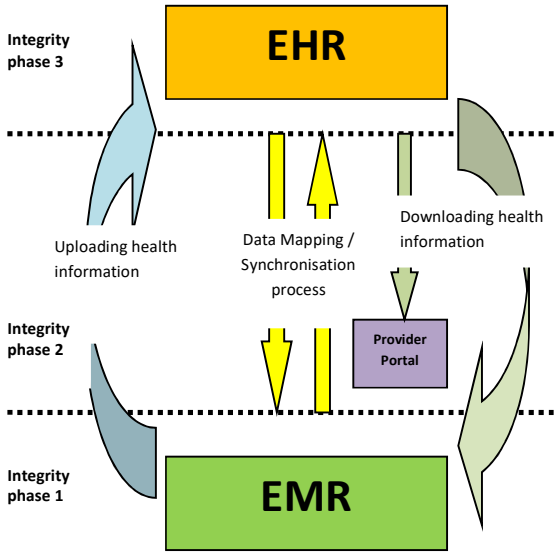


Figure 7: Integrity phases of an EHR system

4.3.1 Integrity phase 1: Ensuring data integrity in Electronic Medical Record (EMR) systems

Garbage-in, garbage-out. The data recorded into medical records that health care providers record must be meaningful and understandable for other health care providers when sharing health information. Otherwise, it will not be useful for other health care providers who access those records when it is necessary. The data integrity must be ensured by providing the right information, at the right time for the right patient to deliver better health outcomes.

Ensuring data integrity in this phase must be carried out by clinical software systems. The data integrity must maintain the use of medical terminology or international medical coding system rather than free text usage in clinically related health information including medical condition and medical history. The coding system must be an option to choose from a pre-developed item list to prevent spelling mistakes. The pre-developed coding system must be linked to international medical approved standards dictionaries and updated regularly, or even daily. The clinical systems that health care providers use in Australia have included

this facility. However, this is deployed as an option and given alternatives to add free texts to clinically related information.

For example figure 8 shown below, is how one of the major primary care provider clinical systems in Australia captures medical history items. There is always an option for clinicians to choose free text. The free text could lead to human errors or spelling mistakes and the impact might be very serious.

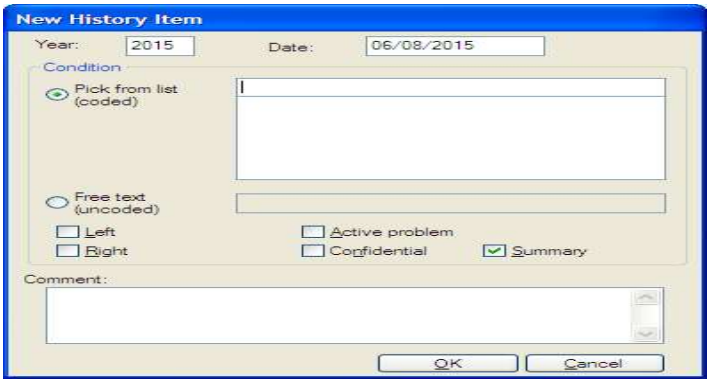


Figure 8: Medical history data capture form

A medical record in an EMR includes various medical-related information of a patient. This information is recorded based on different types of data including patient's contributions, clinical check-up findings, pathology and radiology results, and other measurements. The accuracy of the health data of a patient depends on various inputs. The contribution of a patient is always based on the situation. The health care providers can only record what a patient communicates at the time of the consultation. In other words, a patient can intentionally hide a part of, or complete information from health care providers, they can even provide incorrect data. This integrity concern cannot be resolved unless the patient comes forward and provides the right information.

4.3.2 Integrity phase 2: Ensuring data integrity with linking right records

The communication of health information is a vital part of effective health care. The accurate identification of individuals is critical in all health communication. Mismatching of patients with their records and results is a documented problem for the health system and a clear link has been established between avoidable harm to patients and poor medical records management [123, 28, 29].

As mentioned previously, identifying the right patient at the right time with the right information to upload or download is an essential part of this phase of integrity. To achieve this objective, a standard number (e.g. index) system must be used. The system is intended to assist health care providers to communicate health information with other providers accurately, for example, by providing a more reliable way of referencing patient information electronically.

Moreover, in EHR systems, the delivery of safe, effective and efficient health care relies on good communication and systems that share information, where the subject of care can be reliably and consistently identified. In Australia, the Health care Identifier (HI) number system has been created and automatically allocated to all Australians who were enrolled with Medicare on 1st July 2010 [124].

HI is a unique 16 digit number used to identify patients that help the health care providers to ensure their personal health information is linked with the right person. HIs are the building block for the Personally Controlled Electronic Health Record (PCEHR) system in Australia [125, 126].

Medicare Australia uses the ISO7812 standard to create the HI number to every patient in Australia. The HI number contains, as shown in figure 9 below, a single-digit Major Industry Identifier (MII), a six-digit Issuer Identifier Number (IIN), an Individual Account Identifier (IAI) number, and a single digit checksum based on the Luhn Algorithm. The MII forms the first part of the IIN.

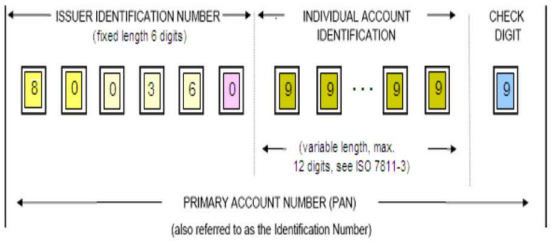


Figure 9: HI number system (Source: [21])

4.3.3 Integrity phase 3: Ensuring data integrity in EHR systems

Improved patient care, increased patient participation, improved care coordination, improved diagnostics and patient outcomes, practice efficiencies, and cost savings are some of the major benefits of the EHRs [127]. However, EHR over the Internet will allow for the exposure of the records to theft and compromise. Personal details in the EHR including full name, date of birth, current address and Medicare number are valuable information for fraudsters to hack. The EHR also leads to deliver information to criminals which could be used to fraudulently obtain prescription drugs. This could have adverse implications for individuals, doctors, and pharmacists whose e-health records are manipulated to facilitate criminal endeavours, where the audit trail will lead back to legitimate users who had access to these records, but who were in no way responsible for their fraudulent manipulation [128].

In 2012, Russian hackers held a Gold Coast medical centre to ransom after encrypting thousands of patient health records [129]. It was not a desktop that was compromised in this example. It was a server that is set up with much more security and rarely used for casual browsing and email. This means the hackers had to get through a firewall, anti-virus scanning software and then administrative credentials on the server.

Considering that recovering from a compromise is a non-trivial exercise, it is likely that these compromises persist for days or weeks, and some machines may remain compromised. Imagine if each of these computers had at least one user who had used it to access their PCEHR. That represents potentially millions of records compromised by online criminals.

That there will be a broad and extensive range of threats must be considered and managed to ensure the integrity of the PCEHR. These may cover the central infrastructure, including core server databases and data processing systems; intermediate data storage and processing systems used by health care professionals and service providers, and the data transport and communications layers, including protocols and channels used for end-to-end or server-to-server communications [128].

The integrity of the information of EHR needs to be trusted to use the system by the health care providers to ensure the success of the initiative. Some health care providers are still concerned about a few integrity issues. For example, the patients who registered with the

PCEHR can hide or completely delete (NOT to modify) the record that their health care providers uploaded for them. This control questions the integrity of the health information of the patient and how confident that the providers can rely on the system to provide health care.

The lack of the sense of shared accountability between system developers and users for product functionality of the EHR can lead to serious integrity issues. The department of health acknowledged to the Office of the Australian Information Commissioner (OAIC) that a technical change had introduced a glitch into the system potentially allowing a handful of health care providers to access PCEHR user's health notes without authorisation, for a short window of time [130].

Chapter 5

Proposed Security Model

The proposed model will be discussed and analysed in this chapter. The discussion and analysis will be based on the findings from the literature review and conceptual approach.

5.1 Proposed security model analysis

The security model has three tiers, with each tier has a different type of security mechanism. Hence, the proposed complete system in this design provides complete security against a different type of threats which can be expected from diverse sources. Table 9 discusses the proposed model with every security level, type of security, the concept used and the protection type that the concept provides.

Table 9: Database security model

Security level	Security type	Concept	Protection type
One	Access control	Log-in pair	Basic entry into the system
Two	De-sensitive data access	Pseudonymisation	Intermediate data access
Three	Cryptography / data encryption	New algorithm	Full data protection

Figure 10 below illustrates the proposed layered model that covers the type of security in every level.

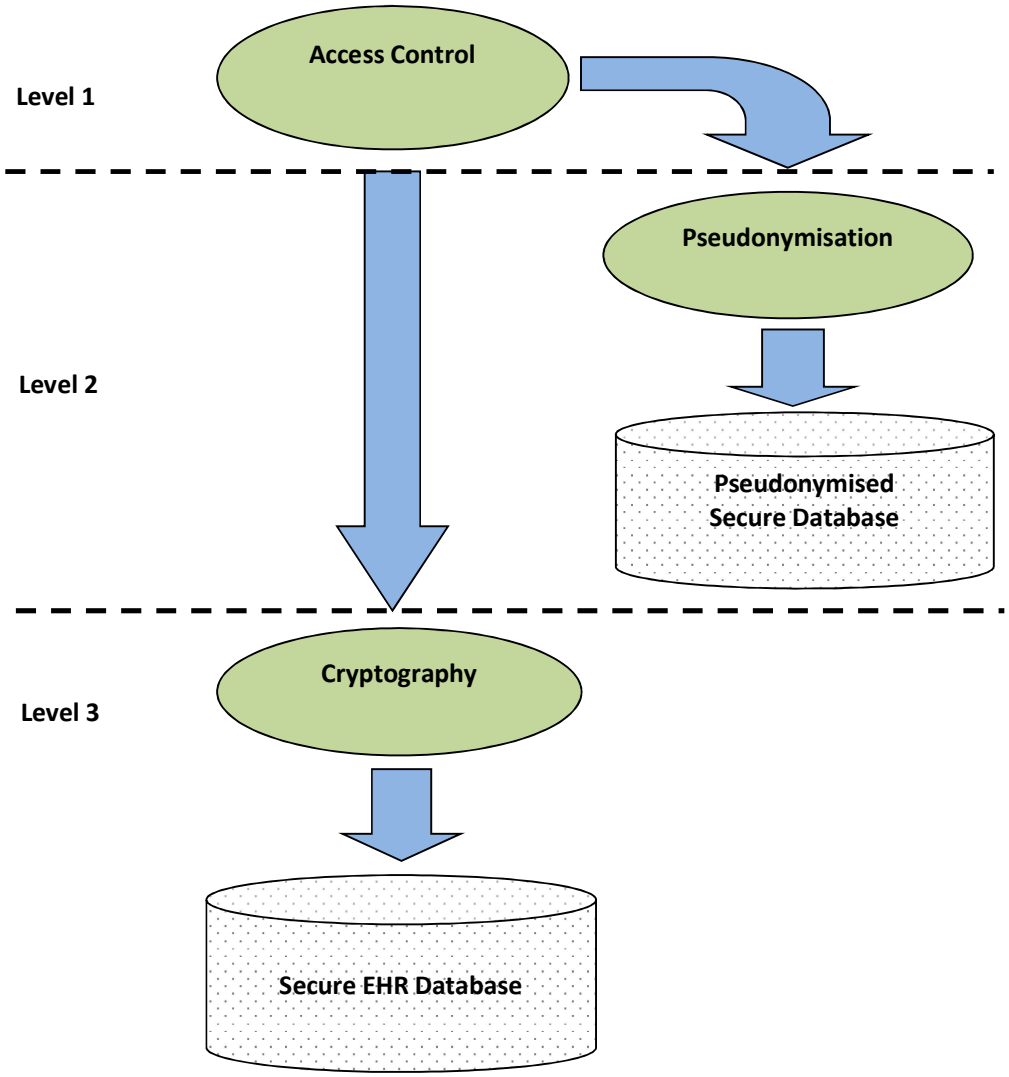


Figure 10: Three levels of the database security model

5.1.1 Security level 1: Access Control

As discussed previously, an access control covers essential services of identification or authentication, authorisation and accountability for a system and their functionalities are;

- Identification or authentication determines who logged in to a system,
- Authorisation provides different privileges for a system by health care employee's job role within a health care organisation and

- Accountability identifies what a subject of user access during his or her log-in.

The Security Engineering Guide (SEG) explains in [18] the term as access control is the traditional centre of gravity of computer security and it is where security engineering meets computer science. The SEG also discusses, in figure 11, how access control works at several levels and describes the following different levels.

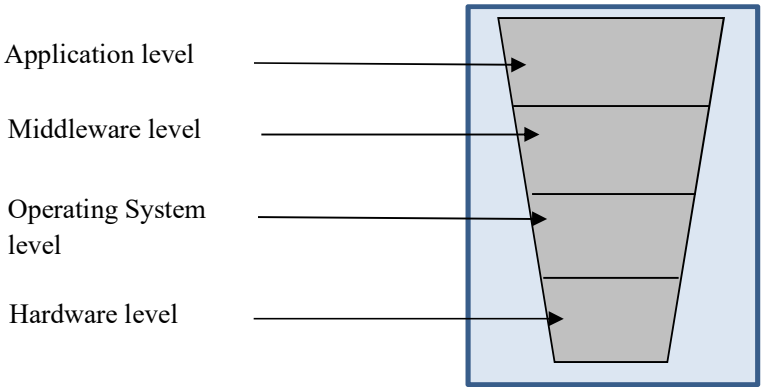


Figure 11: Access controls at different levels in a system [18]

Authentication, authorisation and audit ability and their levels of permits are varied on a different level of access control for a system.

After considering several aspects of access control mechanisms in the literature review, it was realised that there is a real need for improved control on this level of security. Especially in health care settings, the need becomes more prominent. Because of the level of trust within a health care organisation, access rights and privileges are not achieved as expected. In other words, the user privilege access control can be easily breakable or unusable because of the nature of the environment. To enable a strong practice, while strictly following the policies, there should be an advanced method of access control mechanism in place to protect the sensitive information that the organisation holds. The data is the power of any organisation. The data integrity ensures the originality of the data from its source. Therefore, keeping data or information safe and secure is essential in maintaining the data integrity; particularly paramount in health care settings. This led to the development of a mechanism called *log-in pair* which will be an ideal answer to minimise the potential for misuse or abuse of health data within a health care organisation.

The health sensitive and confidential data (e.g.; clinical notes / medical conditions) are stored in databases of the clinical software systems. The current settings, the level of sensitivity of the data and the level of trust within the health care organisation creates a situation where the data is susceptible mostly for internal abuse. Hence, this sensitive data needs to be protected from internal abuse. The *log–in pair* is the technique that can achieve this objective.

Log-in pair is an advanced or improved access control method that is proposed to protect the privacy and confidentiality of the MyHR system in level one. In this method, to enter into the system, two people need to log-in as a pair. To access data from the MyHR using this method, an employee who has the top-level privilege (super-user) has to give authorisation to a user to access health sensitive data. Hence, the super-user can keep track of what the user does with the sensitive data. Every user is made aware that once they log in, the super-user can follow and trace them to keep track of what is being accessed and why (the purpose of the access), it is like a counter check. Responsibility and accountability are shared with this technique. Therefore, this concept will ensure high security. Figure 12 displays the basic concept of the proposed log-in pair model in level one.

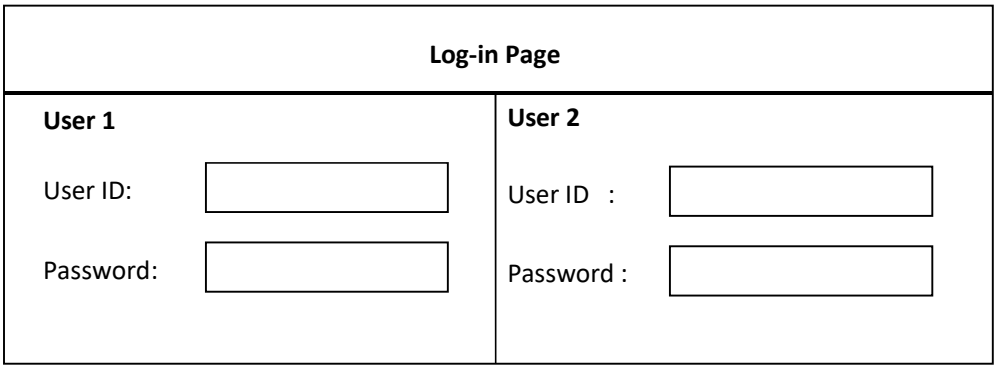


Figure 12: The basic concept of log-in pair

In this method, the employees of the health care provider organisation must be paired with both a user and a super-user. A list of all users and all super-users must be identified. When assigning a pair, there would be some important factors that need to be considered. The factors may include, (i) the geographical location of the users and super-users, for example, both share the same office), (ii) the job discipline of the users - employees who are working in a similar discipline can be paired together, (iii) organisational structure and hierarchy, and (iv) the frequency and time an employee access the system, e.g.; a user who needs to access the system for the whole day, all seven days a week should be paired with another

super-user who is in the long-time accessibility or a work condition rather than pairing with an employee who only needs access to the system for a few hours in a week.

Considering a health care provider organisation with six staff where they all need access to the MyHR system for various purposes and three of them are clinicians including two doctors and a nurse. The rest of the team (three staff) includes admin staff that assists the practice with their business, need also access the MyHR to call patients for recalls and reminders. Every user has his (or her) own individual user id and password to enter into the system. For instance, when considering pairs A and B, C and D and E and F, in the pair log-in concept, for user A to enter into the system then both user A and user B should enter their user id and password which are different to each other. Similarly, if another user needs to enter into the system, then his or her user partner (i.e., a super-user) should also agree and give permission.

When considering the pairs design stage, the users who may be using the MyHR system (A, B, C, D, E & F) can be categorised as follows in table 10 for a health care organisation.

Table 10: Design log-in pair user

Pair	User	Super user
1	A	B
2	C	D
3	E	F

This is a basic example of the design. In practicality, this can involve more users and more super-users. Also, there will be instances where a user relies on more than one super-user considering the unavailability factor when the user requires permission. Therefore, the log-in page must be designed to accept inputs from two users that include their user IDs and passwords that are not identical. The system also verifies that a super-user who permits a user is accepted and predefined in the allocation table. In this way, the security assurance can be provided with this system that one user cannot enter into the system on his (or her) own to access the sensitive health information in the MyHR system. If one employee needs to enter into the system, he (or she) is aware that the partner super-user who is allocated for

the session will also have accountability. Hence, this shared accountability opportunity helps to prevent sensitive information from internal misuses.

However, in practicality, this system also has its problems. The following are some of the issues identified and discussed.

(i) If one user who needs to give permission is absent. For example, in the above table, if user B is on leave, then user A cannot enter into the system or perform his (or her) routine activities.
(ii) The system cannot prevent if both in a pair together decide to abuse the health data.
(iii) Having someone else to log in at the same time as another user creates potential sources of bottleneck and make the system unavailable or unused.
(iv) If doctors and nurses are potential *gatekeepers* (the authorising login), these professions are already extremely busy, and likely to create users circumventing the system.
(v) If authorising persons regularly logon and give the login credentials to users, then this defeats the whole purpose of the system.

To overcome the first problem, a super-user may be able to permit via the Internet or networking as future development. Alternatively, practice managers will also be considered as super-users who can permit users to work on sensitive data. Another option might be that the permission can be given by more than one super-user. For example, the revised log-in pair user table is shown in table 11 below. In this revised table, super-users B, X and Y can permit user A. The users X and Y may be the management staff members who do not access to the MyHR system but both can permit users on behalf of the organisation to complete the user's daily functions. An example of this might be a practice manager and/ or office manager.

Table 11: Revised design log-in pair users

Pair	User	Super-user
1	A	B or X or Y

2	C	D or X or Y
3	E	F or X or Y

However, it is very difficult to overcome the second problem. A system monitoring facility may be developed as the further deployment of this system to monitor the users and super-users. A system audit and/or quality improvement process may mitigate this risk. The system itself must be notified and does not give access to other users to avoid bottlenecks and unnecessary delays in logging on the system over the network.

In the health care organisation environment, doctors and nurses are extremely busy and difficult to contact to gain their login to access the system. However, they are the people who have got authorisation to access clinical information in health care settings. To resolve this issue in creating users circumventing the system, alternative non-clinical top-level staff can be appointed (i.e.; practice manager, assistant practice manager or office manager). Super-user authorisation is a crucial part of this method. Therefore, the login credentials of super-users must be strong and changed periodically. Considering the super-user's availability, the system can be configured to send an auto-creating password for the super-user through an email or a text message to the user's mobile phone on a regular basis, maybe daily. Another control may be that the super-user can log in to the system utilities using their member password (which is different from authorisation password process) and view the daily authorisation options. In other words, a super-user can provide predefined permission according to his or her circumstances. For example, a super-user goes on a week holiday and then he or she will be able to go to the system utility and select a free-password option for the week for the users. This temporarily alternative option gives users a flexible setting under a strict condition.

Once a user logged in using his or her credentials, the system will send a message or alert to the allocated super-user that permission is pending. The communication exchange can be performed using an existing mobile security service, the same computer setup or different computers that are connected via a network. There will be a certain time limit that the permission must be given by the super-user. For example, once a user logged in, then the allocated super-user must provide permission within 60 seconds. If the first super-user fails to permit within that time frame, then the system sends the message to the second allocated super-user. If the second user also fails to permit within 60 seconds, it will finally

go to the third super-user. If all attempts fail, then the request session will come to an end and the user cannot access the system.

Once the super-user is determined that there is permission waiting for his or her approval to enter into the system for the user, the message must be sent out through an effective communication line to and from as quickly as possible. This speedy process can be completed using an existing 'mobile security system'. A mobile security system will be the best solution for this communication channel of the proposed model. Once the mobile security two-factor authentication is enrolled the user can log in as usual with their username and password to access the MyHR system and then the super-user will receive a message through the device for the permission. This process can be done via SMS, voice call, one-time passcode or mobile smartphone apps. For example, *Duo* mobile security system [351] has its smartphone app to do the two-factor authentication verification process. The system also lets users link multiple devices to the account such as a mobile phone and a landline, a landline and hardware token or two different mobile devices [351]. This will provide increased accessibility for the super-users. As mentioned in Figure 5 below, the mobile security system will provide an additional security layer for the MyHR system. The username and password that has been created for the system remain the same and once it is provided, the super-users' approval request will be sent out to the super-user preferred communication device/s. Consequently, if a user wants to access patients' sensitive health information for any reason (e.g. follow up or targeting high chronic disease patients to send a reminder), then an authorised person (super-user) must give the permission. Figure 13 below shows how a mobile security system works with a two-factor authorisation verification process [78 – Author's previous publication].

Figure 13: How a mobile security system works (source: [351])

When creating a user login for a user to access past medical history using clinical software, a super-user link must be established as illustrated through the computer program coding. Moreover, a super-user has more than one option to approve or deny the user login request. For example, the following options are available with the *Duo* mobile security system.

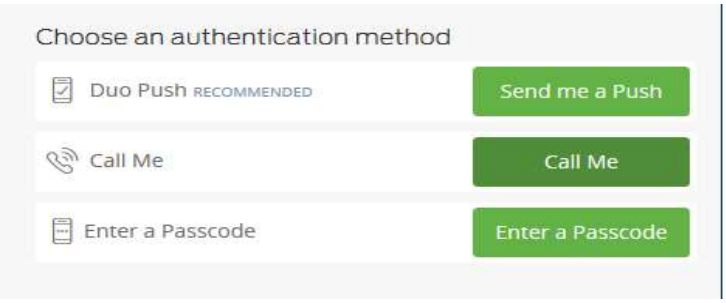


Figure 14: Authentication methods for mobile security system

Figure 14 above illustrates the three various options available with *Duo* mobile security systems for a user to receive a response from a super-user. According to these options, a super-user can set the mobile security option how they want to permit either by pushing a button, calling or entering a passcode. This preference also makes the system more effective as the super-user concerns the time.

5.1.2 Security Level 2: An Intermediate State of Database (ISD)

A previous work that the author published in research papers, may also be discussed in this section.

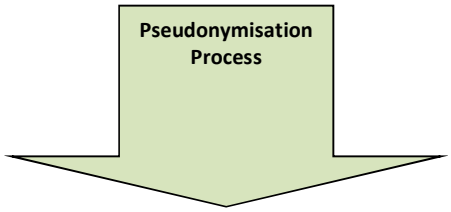
In the proposed model, security is being established at three different levels. Level 1 is the establishment of access control (log in) via the introduction of the *log-in pair* system which has been described in section 5.1.1. The Level-3 is cryptography (encryption and decryption technique) which will be described in section 5.1.3. In this section, the necessity, rationalisation, and process of *middle level 2* are being described.

When Level 1 (access control) and Level 3 (Cryptography – encryption and decryption) security measures were looked at in detail, it was obvious that they will not meet the purpose of securing data in the area of Business Intelligence (BI) because they only permit "all or nothing" access. Generally, in many health care organisations, employees are given access to sensitive information to perform the day to day work such as identifying patients for a health check, processing documents, analysing trends or even testing and maintaining eHealth systems. An employee accessing the sensitive data during routine work is the main reason for putting the privacy and security in high risk where sensitive data can be abused internally. However, the employees could perform their routine works just as effectively with de-sensitised data where the critical sensitive data are some or other *blinded*.

This led to the thought for developing an Intermediate Security Level (Level 2) where it permits health care employees to access the required data for routine work but prevents them from viewing the sensitive data linked to these records. This security level will allow the employees to access the data for routine work such as identifying patients for any reason including targeting chronic disease or a health check, processing documents, analysing trends and testing and maintaining eHealth systems without any need for them to view any sensitive data. Using the *pseudonymisation* technique patients' personally identifiable fields including name and health care identifier within a health data record are replaced by one or more artificial (meaningless) identifiers which are called pseudonym as shown in table 12 below [354 - Author's previous publication].

Table 12: The basics of pseudonymisation technique

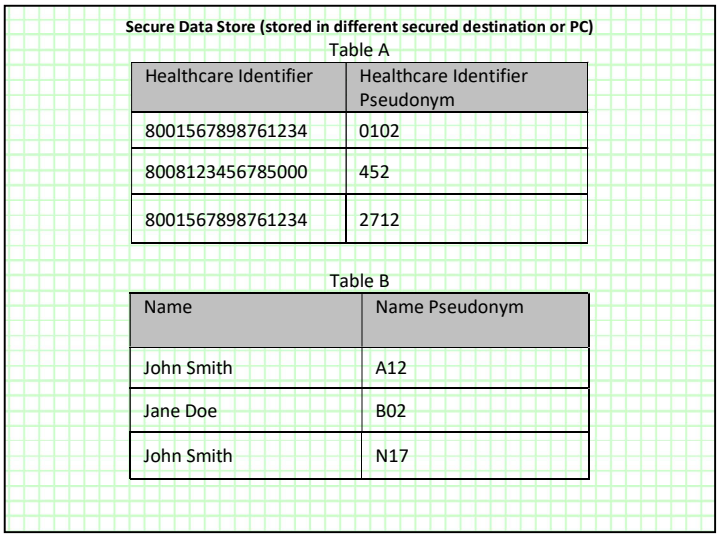
Health care Identifier	Medication	Date	Condition	Name
8001567898761234	Insulin	01-10-2014	CD	John Smith
8008123456785000	Dapotum	05-10-2014	MH	Jane Doe
8001567898761234	Thalitone	10-10-2014	CKD	John Smith



Health care IdentifierPseudonym	Medication	Date	Condition	Name Pseudonym
0102	Insulin	01-10-2014	CD	A12
452	Dapotum	05-10-2014	MH	B02
2712	Thalitone	10-10-2014	CKD	N17

With this technique, a user can still search data for relationships, however, it cannot capture all the value of the data. On the other hand, copying *pseudonymised* data is similarly pointless as the keys connecting the valuable links between the accessible pseudonym and the actual data itself are held elsewhere as shown in Table 13 below [354 - Author's previous publication].

Table 13: Hidden index data set



Secure Data Store (stored in different secured destination or PC)

Table A

Healthcare Identifier	Healthcare Identifier Pseudonym
8001567898761234	0102
8008123456785000	452
8001567898761234	2712

Table B

Name	Name Pseudonym
John Smith	A12
Jane Doe	B02
John Smith	N17

The hidden connective index data is stored in a secure destination or in another workstation where the ordinary users cannot be accessed.

The difference between encryption and *pseudonymisation* is; encryption or password permission exposes sensitive data and relationships. However, in *pseudonymisation*, the sensitive data is hidden and the relationships are exposed. The two key requirements for *pseudonymisation* are; data patterns must be maintained for linkage or analysis and personal data that will be shared, either internally or with a partner, must be hidden during the usage. Thus, adopting the *psudonymisation* technique to the record will preserve privacy and reduce risk exposure and mitigate any potential impact of internal and external security breaches. Furthermore, the *Pseudonymisation* renders stolen data effectively useless for identity theft and other fraud. This facilitates secure outsourcing and offshoring by using de-identified data to identify health records. The health care organisations can attain cost savings whilst significantly reducing the security concerns of using third party processors [354 - Author's previous publication].

The health software system integrators, developers and systems administrators can use de-identified data for estimating eHealth projects that work with health sensitive data, designing and testing new systems that source health sensitive data from existing operations and maintaining eHealth systems that manipulate sensitive data. The health care identifiers and other health-related number systems including Medicare effectively become

sensitive through their long term usage. An effective *pseudonymisation* solution can assign and maintain new pseudonyms for these sensitive identifiers as illustrated in tables 13 and 14 [354 - Author's previous publication].

In this technique, the security level-2 provides an intermediate step between "all or nothing" access, which effectively reduces the risk of internal abuse of sensitive data. It enables the identification of individuals and their records, without exposing the individual's health sensitive information. Also, this level of security maintains privacy for the analysis, testing and sharing of data where the data relationships are critical, such as in Business Intelligence Systems (BIS) and Decision Support Systems (DSS). It also facilitates analysis work with audited health data. When required, data can be given to link back to each sensitive value [354 - Author's previous publication].

The literature review on this area repeatedly brought the name of a company called *Sapior*. It has been stated that this company is developing this kind of security system which the company has labelled as *pseudonymisation*. The company's website (www.sapior.com) has mentioned that the U.K. information commissioner recommends the use of *pseudonymisation* to protect sensitive patient information in the records kept by the National Health Services (NHS) system. Currently, Sapior is in the process of maintaining the security level for NHS using the *pseudonymisation* technique [19, 355].

4.1.2.1 Pseudonymisation

Adopting a pseudonym technique for health records will preserve privacy. In the pseudonymisation model, while the sensitive health data is protected, the users of the system are allowed to access to insensitive or less sensitive elements in the records. This method manages the sensitive data by replacing critical data components with a code or notifications that are known as pseudonyms. The uses that access the information cannot view the data itself because it has no direct accessibility for them, only the certain components of the information related to a request are returned to the user. The consequence of the *pseudonymisation* method is that while the users can still pursuit data for its relationships, the users cannot identify all the value of the data. Therefore, this technique ensures the users that external to the actual context of the services cannot view and/ or alter the data in an unauthorized manner. Also, simply copying *pseudonymised* data is similarly useless as the keys linking the useful relations among the available pseudonym and the real data itself are stored in another place away from this location. Thus, with this

technique, the sensitive data is concealed and the relationships between the data are visible. Two key requirements that exist with this technique are;

1) The data patterns are retained for relationships and analysis
2) Sensitive data that is shared, either internally or externally with a partner, is concealed during the access.

The NHS utilises the *pseudonymisation* method to preserve the privacy of the sensitive health records in the U.K. The health care organisations can obtain a wide range of benefits of using this method [19]. The method reduces the conceivable threats possibilities and possible damage that can occur from inside and outside security breaches. The impact of risk of loss or theft data is unusable for any fraud including personal identity. In outsourcing and offshoring opportunities, the process promises in sharing the de-sensitised data of personal and sensitive information like health records. Therefore, using this method, while the health care organisations achieve cost-effectiveness, it considerably decreases the security distress of using third party services such as outsourcing and offshoring. The external users such as system integrators, software developers and systems operators can use the de-sensitised data for various purposes that they involve within their job roles including assessing projects that deal with sensitive data, improving organisation's performance, designing and testing new software applications that work with sensitive data, and preserving IT systems that operate sensitive data. The method also provides an opportunity where all staff members can use the data without the risk of threats while the data sensitivity is protected from intrusive or unwitting workers within an organisation. In health records, the *Pseudonymised* data will minimise the audit requirement and facilitate sharing initiatives, whilst exposing trends and protecting sensitive information. The health care identifier and Medicare numbers also become sensitive because of their long term usage. A health record also includes these kinds of personal data in addition to health-related clinical information. A better *pseudonymisation* solution can preserve privacy by replacing new pseudonyms for these sensitive identifiers as required. This is critical for any health care provider organisations to preserve such systems and other clinical related software applications that deal with patients' sensitive data in maintaining business continuity.

5.1.3 Security Level 3: Cryptography / Data Encryption

Even though a final working protocol is not one of the objectives in the scope of this project, leading the way to implement such systems would be more beneficial for future development.

In the three-layered security model, in addition to improved access control mechanisms and *pseudonymisation* technique, there is a need to encrypt and store data to reduce the privacy and security risks around the system. The stored data is more vulnerable to threats and data breaches. Moreover, the patients' sensitive data stored in the cloud becomes susceptible to current trends. Therefore, ensuring a high level of security for those data is paramount. The cryptography data encryption can be the most appropriate security method of several others. Encryption of stored data can, consequently, be a key technique in preventing or restricting information theft, even in the situation where the access controls are bypassed.

5.1.3.1 Cryptography Algorithms Overview

First of all, it is very important to analyse the existing cryptography algorithms and cryptanalysis to reach a strong algorithm for the third tier to ensure high security in the proposed protocol. To achieve this objective, the following existing algorithms are being discussed. To explicit the proposed protocol and the objective of the research, two basic cryptography algorithms are discussed. The weaknesses of those two algorithms are identified and analysed comprehensively in addition to the discussion of those methods. Further development and/ or solutions are determined and implemented to overcome those weaknesses to achieve the objectives of this research. To achieve this objective, a substitution cipher and symmetric encryption technique are considered. Even though the substitution cipher and symmetric encryption algorithms are not considered as the new techniques and not in use currently, identifying and overcoming the weaknesses of those methods will form a new algorithm that can provide high security. Therefore, the substitution cipher and symmetric encryption techniques and the weaknesses of the models are discussed in-depth and provided potential solutions for those weaknesses. The advanced model with the solutions for weaknesses of existing techniques, ultimately, will produce a new concept that contains high security. Furthermore, the combination of both substitution cipher and symmetric encryption technique algorithms represent both data encryption techniques such as substitution and transformation. This is another reason why

the combination of both techniques is used to achieve a strong algorithm as the third level of the proposed model.

5.1.3.2 Substitutions Cipher

In cryptography, the substitutions cipher is a simple and most broadly used encryption method. A widely used substitution cipher is Caesar cipher. In this method, each letter in the plaintext is interchanged by another letter with fixed numeral positions in the alphabet. For instance, in figure 15 below, the letter *A* would be interchanged by *D*, the letter *B* would be replaced by *E*, the last letter *Z* would become *C* and so on. In this example, the letter shifts by the fixed position of three.

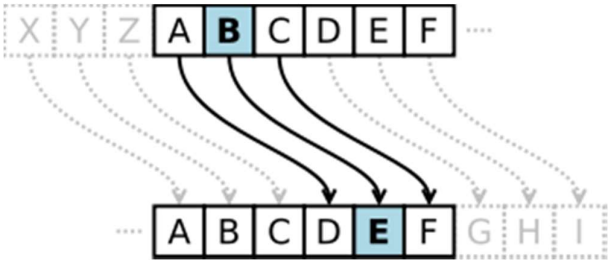


Figure 15: The basics of substitutions cipher

(Reproduced from F.L. Bauer, Decrypted Secrets, 2nd edition, 2000, Springer)

The transformation of letters can be replaced by any fixed number positions; even the positions interchange both side rotations whether left or right of the alphabet. For example, a Caesar cipher substitution that uses a right rotation of five is shown below. In this example, the alteration parameter is five which is used as the key.

Plain: ***A B C D E F G H I J K L M N O P Q R S T U V W X Y Z***

Cipher: ***F G H I J K L M N O P Q R S T U V W X Y Z A B C D E***

Using this method, to make a message secure, simply check every letter of the original message that is known as *plaintext* and markdown the corresponding letter in the *ciphertext* line. To bring back the original *plaintext*, look up the replaced letter and move in the other direction of fixed number places that moved to make encipher and transform. The following example simply explains the method, the key is five.

Plaintext: **come for a meeting tomorrow**
Ciphertext: **HTRJ KTW F RJJYNSL YTRWWTB**

Using modular arithmetic method by transforming the letters into numbers, the encryption can be expressed in an algorithm. Considering a model of A = 0, B = 1,….. Z = 25 representation with the letter is X and the shift is *n,* the encryption algorithm would be described mathematically as follow;

En (X) = (X+n) mod 26

Considering the similar parameters, the decryption algorithm would be;

Dn (X) = (X-n) mod 26

A different definition can be given for modulo operations. In this method, the result is in the range between 0 and 25. In other words, if the result of X+*n* or X-*n* is not in the range between 0 and 25, then it has to be subtracted or added by 26. However, the transformation remains the same throughout the message, so the cipher is classed as a type of *monoalphabetic substitution* as opposed to *polyalphabetic substitution.*

The following drawbacks are identified as the weaknesses of this algorithm [17]:

(i) The encryption and decryption algorithms are known
(ii) There are only 25 keys to try
(iii) The language of the *plaintext* is known and easily recognisable
(iv) Easily breakable using frequency analysis

5.1.3.3 Symmetric encryption technique

It is a manual symmetric encryption technique developed by Charles Wheatstone for telegraph secrecy and known as Playfair [20]. It was the first literal digraph substitution cipher. The technique encrypts pairs of letters (it is called digraphs), instead of single-letter [21]. The Symmetric encryption technique is significantly harder to break since straight frequency analysis doesn't work with it. The frequency analysis is a method for breaking simple substitution ciphers. It is a primitive algorithm block cipher in the modern standards now. The computational power of today's computers can break it easily by using quality software. But after its creation, it was adopted by the British Government to use in its official messaging. However, the dogma used by Symmetric encryption technique cipher

is used as a baseline for many modern computer block ciphers [22]. In this perspective, using this technique as a foundation for this research and development is appropriate.

(i) How does the symmetric encryption technique algorithm work?

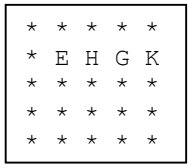
1. A key is selected that will be used in creating the Playfair matrix.

2. Playfair matrix is a 5 * 5 matrix consisting of all alphabets in such a way that no letter should repeat in it with I and J treated as one letter. The selected cipher key is important as it helps in creating matrix and encoding, decoding of the message. The key must be private and be known by both the sender and receiver to encode the messages.

3. After choosing a key, the message is delivered in the form of digraphs in such a way that no digraph consists of a similar letter. If so, replace the repeated letter with some other letter like 'X'.

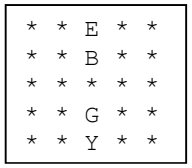
4. In the next step, the digraph is replaced with the encoded pair of letters from the matrix. Each digraph will be replaced with a specific pair of the matrix. The following rules are applied in replacing the original digraph.

   a. If the letters appear in the same row of the matrix, replace them with the letters to their immediate right respectively.



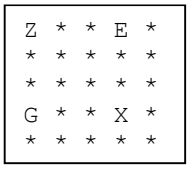
EG ⟶ HK

   b. If the letters appear on the same column of the generated matrix, replace them with the letters immediately below respectively.



EG ⟶ BY

c. If the letters are not on the same row or column, replace them with the letters on the same respectively but at the other pair of corners of the rectangle defined by the original pair [21].



EG ⟶ ZX

(ii) An example of a symmetric encryption technique algorithm

Key – *WHEREISTHAT*

Message – *Come for a meeting tomorrow*

Using this *Playfair* example as the key, the matrix table is displayed in table 14.

Table 14: Playfair matrix table

W	H	E	R	I
S	T	A	B	C
D	F	G	K	L
M	N	O	P	Q
U	W	X	Y	Z

Therefore, encrypting the message *come for a meeting tomorrow* would be;

CO ME FO RA ME ET IN GT OM OR RO WX

Hence, the following transformation can be occurred for the above digraph:

The pair CO forms a rectangle and the diagraph would be ***CO*** ⟶ ***AQ***

The pair ME forms a rectangle and the diagraph would be ***ME*** ⟶ ***OW***

The pair FO forms a rectangle and the diagraph would be ***FO*** ⟶ ***GN***

The pair RA forms a rectangle and the diagraph would be ***RA*** ⟶ ***EB***

The pair ME forms a rectangle and the diagraph would be ***ME*** ⟶ ***OW***

The pair ET forms a rectangle and the diagraph would be ***ET*** ⟶ ***HA***

The pair IN forms a rectangle and the diagraph would be ***IN*** ⟶ ***HQ***

The pair GT forms a rectangle and the diagraph would be ***GT*** ⟶ ***FA***

The pair OM is in the same row and the diagraph would be ***OM*** ⟶ ***PN***

The pair OR forms a rectangle and the diagraph would be ***OR*** ⟶ ***PE***

The pair RO forms a rectangle and the diagraph would be ***RO*** ⟶ ***EP***

The pair WX is in the same row and the diagraph would be ***WX*** ⟶ ***YZ***

The message *come for a meeting tomorrow* becomes

"***AQOWGNEBOWHAHQFAPNPEEPYZ***"

(iii) The strengths of symmetric encryption technique

- It is simple to operate and understand.
- Only one key is required to be remembered by both the sender and receiver.
- The substitution of the letter depends on the key selection. The 5*5 matrix is generated according to the key, thus, the plain text digraph is replaced with different *ciphertext* digraph and different key selection. It results in improved security of the algorithm.
- Simple cryptanalysis techniques may not work easily to break it.

(iv) The weaknesses of symmetric encryption technique

- No encryption of the numeric data or punctuation symbols
- The encrypted message can be crashed by frequency analysis.

5.1.3.4 The proposed algorithm: HighSec algorithm

Part of this development is discussed and published in one of the author's research work.

The proposed algorithm has been named as *HighSec*. Based on the study, the following matrix table has been designed to the *HighSec* algorithm for substitution purposes.

The newly designed *HighSec* substitution secret fixed (HSSF) table is shown in table 15 that needs to be used in the new algorithm.

Table 15: *HighSec* substitution secret fixed (HSSF) table

A	***B***	***C***	***D***	***E***	***F***	***G***
39	40	41	42	1	2	3
H	***I***	***J***	***K***	***L***	***M***	***N***
4	5	6	7	8	9	10
O	***P***	***Q***	***R***	***S***	***T***	***U***
11	12	13	14	15	16	17
V	***W***	***X***	***Y***	***Z***	***0***	***1***
18	19	20	21	22	23	24
2	***3***	***4***	***5***	***6***	***7***	***8***
25	26	27	28	29	30	31
9	***_***	***?***	***@***	***,***	***.***	***&***
32	33	34	35	36	37	38

(i) How does the *HighSec* algorithm work for encryption

The *HighSec* algorithm is explained in seven steps with suitable examples

Plain Text – **DO NOT USE 100PC**

Key – **TABLE@7**

Step 1:

Split the plaintext message into five-character groups. Use X's to fill in the last group.

So the message "**DO NOT USE 100 PC**" then the plaintext is;

DO NOT USE10 0PCXX

Step 2:

Split the key into five-character groups. Use the characters which belong from the number 1 onwards (ie; E, F, G, H…..) to fill the equal number of groups as the plaintext.

So the key "**TABLE@7**" will be;

TABLE @7EFG HIJKL

Step 3:

Convert the ***plaintext*** message from characters into a numbers using the above matrix table

42 11 10 11 16 17 15 1 24 23 23 12 41 20 20

Step 4:

Convert the ***key*** characters into number using the above same matrix table

16 39 40 8 1 35 30 1 2 3 4 5 6 7 8

Step 5:

Add the plaintext number to the key numbers, modulo 42. For example, 1+1=2, 42+1=43, and 43-42=1, so 42+1=1.

16 8 8 19 17 10 3 2 26 26 27 17 5 27 28

Step 6:

Convert the numbers back to characters using the same matrix table.

TLLWU NGF33 4UI45

Step 7:

Split into two-character groups. Fill the gap by 'X'.

TL LW UN GF 33 4U I4 5X

Step 8:

If there is more than one character repeating in a group, fill by "_" and move the second repeat character by one place, which will result in

TL LW UN GF 3_ 34 UI 45

Step 9:

Improved symmetric encryption technique algorithm will be applied at this point as step 9:

Improvements:

1. Increase in the size of the matrix from 5*5=25 to 7*6=42
2. Inclusion of the digits 0-9 and widely used punctuation symbols like _ ?& . , @
3. Separate use of letters I and J

How does the improved symmetric encryption technique algorithm work.

1. The algorithm works similarly to the symmetric encryption technique cipher. The first step is to select a key that will be used in creating the 7*6 matrix. The matrix will contain alphabets A-Z, number 0-9 and punctuation symbols (space &, . @ ?) in such a way that no letter should repeat. The selected cipher key is important as it helps in creating matrix and encoding, decoding of the message.
2. The key may or may not be private but should be known to both the sender and receiver to encode and decode the message.

3. After choosing a key, the message will be divided into pairs in such a way that no digraph consists of a similar character. If so, replace the repeated letter with white space.
4. The next step is to replace the diagraphs with the encoded pair of letters from the matrix according to the size of the selected key. Each digraph will be replaced with a specific pair from the matrix. Following rules are applied to replace the original digraph:
    a) Calculate the size of the selected key.
    b) If the characters appear in the same row of the matrix table, replace them with the characters where the total size of the key places away to them respectively on the right side. This change will make it different from the original symmetric encryption technique algorithm rules.
    c) Similarly, if the letters appear on the same column of the generated matrix, replace the characters where the total size of the key places away downwards respectively.
    d) If the letters are not on the same row or same column, replace them with the character on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

Use the improved *symmetric encryption technique* diagram to replace the above character set. The length of the key is 7. Thus, based on the key, the following matrix table (Table 16) will be created.

Table 16: *HighSec* Matrix

T	**A**	**B**	**L**	**E**	**@**	**7**
F	**G**	**H**	**I**	**J**	**K**	**M**
N	**O**	**P**	**Q**	**R**	**S**	**U**
V	**W**	**X**	**Y**	**Z**	**0**	**1**
2	**3**	**4**	**5**	**6**	**8**	**9**
_	**?**	**,**	**.**	**&**	**C**	**D**

The message "**TL LW UN GF 3_ 34 UI 45**" will be;

So the following replacement can be occurred for above digraph:

The pair TL in the same row, thus **TL** ⟶ **TL**

The pair LW forms a rectangle, thus **LW** ⟶ **AY**

The pair UN in the same row, thus **UN** ⟶ **UN**

The pair GF is in the same row, thus **GF** ⟶ **GF**

The pair 3_ forms a rectangle, thus **3_** ⟶ **2?**

The pair 34 is in the same row, thus **34** ⟶ **34**

The pair UI forms a rectangle, thus **UI** ⟶ **QM**

The pair 45 is in the same row, thus **45** ⟶ **45**

The final *ciphertext* is; **TL AY UN GF 2? 34 QM 45**

Therefore, the *ciphertext* for the Plain Text "**Do Not Use 100PC**" will become;

TLAYUNGF2?34QM45

The encryption process is illustrated with block diagrams in figure 16. This step by step process shows the framework to build the new encryption algorithm. Additionally, the steps are also explained with examples. The clear instruction will assist to develop the proposed protocol.

(ii) Encryption framework using the *HighSec* algorithm

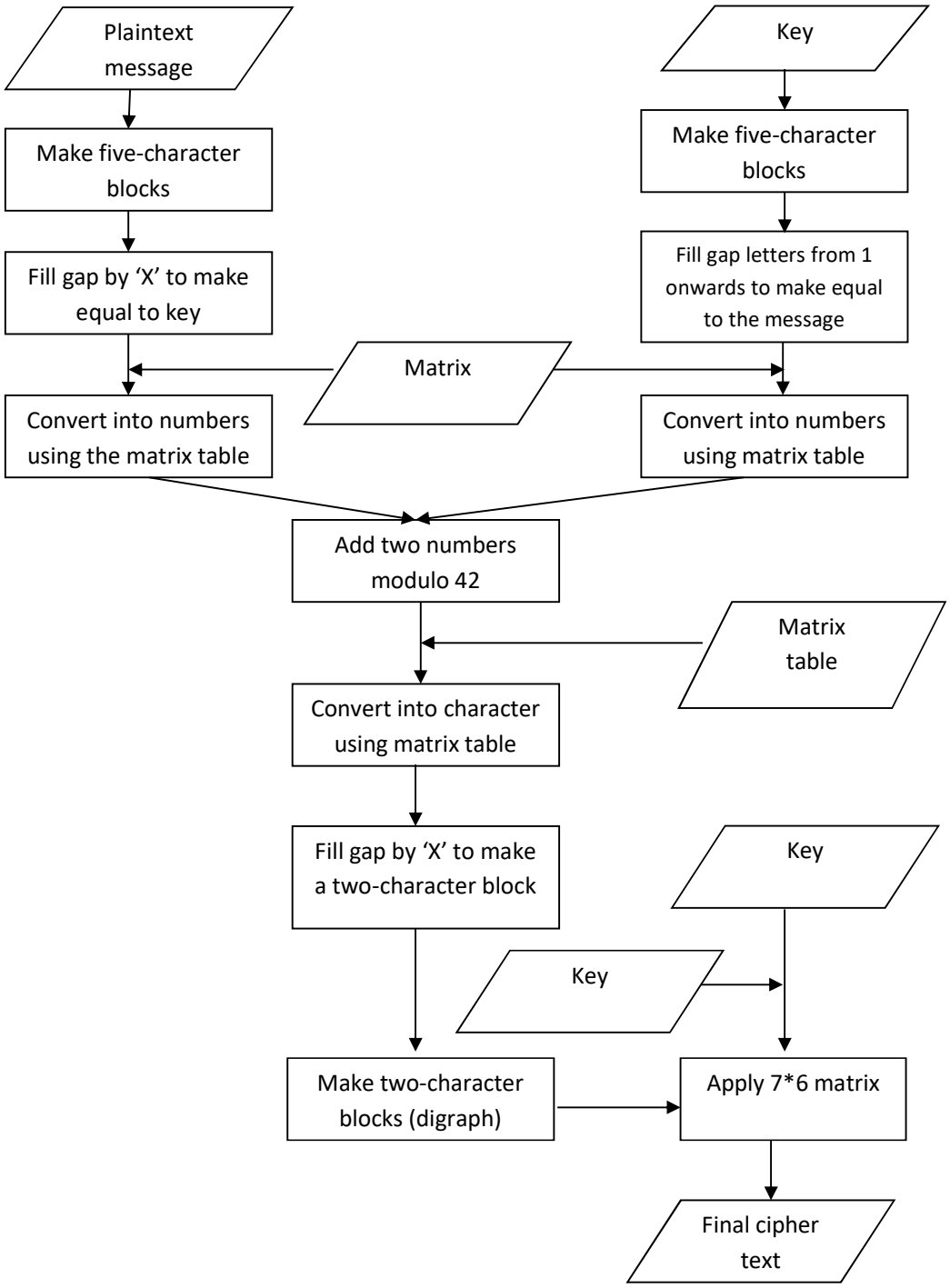


Figure 16: *HighSec* block diagram for encryption

(iii) How the *HighSec* algorithm works for decryption

Step 1 :

Make the final cipher text *"**TLAYUNGF2?34QM45**"* as two-character blocks. So the cipher text will be;

TL AY UN GF 2? 34 QM 45

Step 2:

Apply 7*6 matrix table to convert into alternate two-character blocks for the cipher text "**F_B3WMGF2?34ZD45**":

So the following replacement can be occurred for above digraph:

The pair TL is in the same row, thus **TL** ⟶ **TL**

The pair AY forms a rectangle, thus **AY** ⟶ **LW**

The pair UN is in the same row, thus **UN** ⟶ **UN**

The pair GF is in the same row, thus **GF** ⟶ **GF**

The pair 2? forms a rectangle, thus **2?** ⟶ **3_**

The pair 34 is in the same row, thus **34** ⟶ **34**

The pair QM forms a rectangle, thus **QM** ⟶ **UI**

The pair 45 is in the same row, thus **45** ⟶ **45**

The result will be; ***TL LW UN GF 3_ 34 UI 45***

Step 3:

If there is any "_" in the two-character block in step 2 just remove it. So the result in step 3 is;

TLLWUNGF334UI45

Step 4:

Make the characters into five-character blocks and convert into numbers using the above matrix table

16 8 8 19 17 10 3 2 26 26 27 17 5 27 28

Step 5:

Convert the key "TABLE@7" characters into number and fill the gap to make an equal number of the result in step 4 from 1 onwards using the above same matrix table

16 39 40 8 1 35 30 1 2 3 4 5 6 7 8

Step 6:

Subtract result cipher text number in step 4 from the key number in step 5, modulo 42.

42 11 10 11 16 17 15 1 24 23 23 12 41 20 20

Step 7:

Convert the numbers back to characters.

DO NOT USE10 0PCXX

Step 8:

Remove the 'X's at the end and get the final message.

DONOTUSE100PC

Therefore, the final message is; ***DONOTUSE100PC***

This means, both the encryption and decryption process work and are verified.

The decryption process is illustrated with block diagrams in figure 17. This step by step process shows the framework to build the new decryption algorithm. Additionally, the steps are also explained with examples following the diagram.

iv) Decryption framework using the *HighSec* algorithm

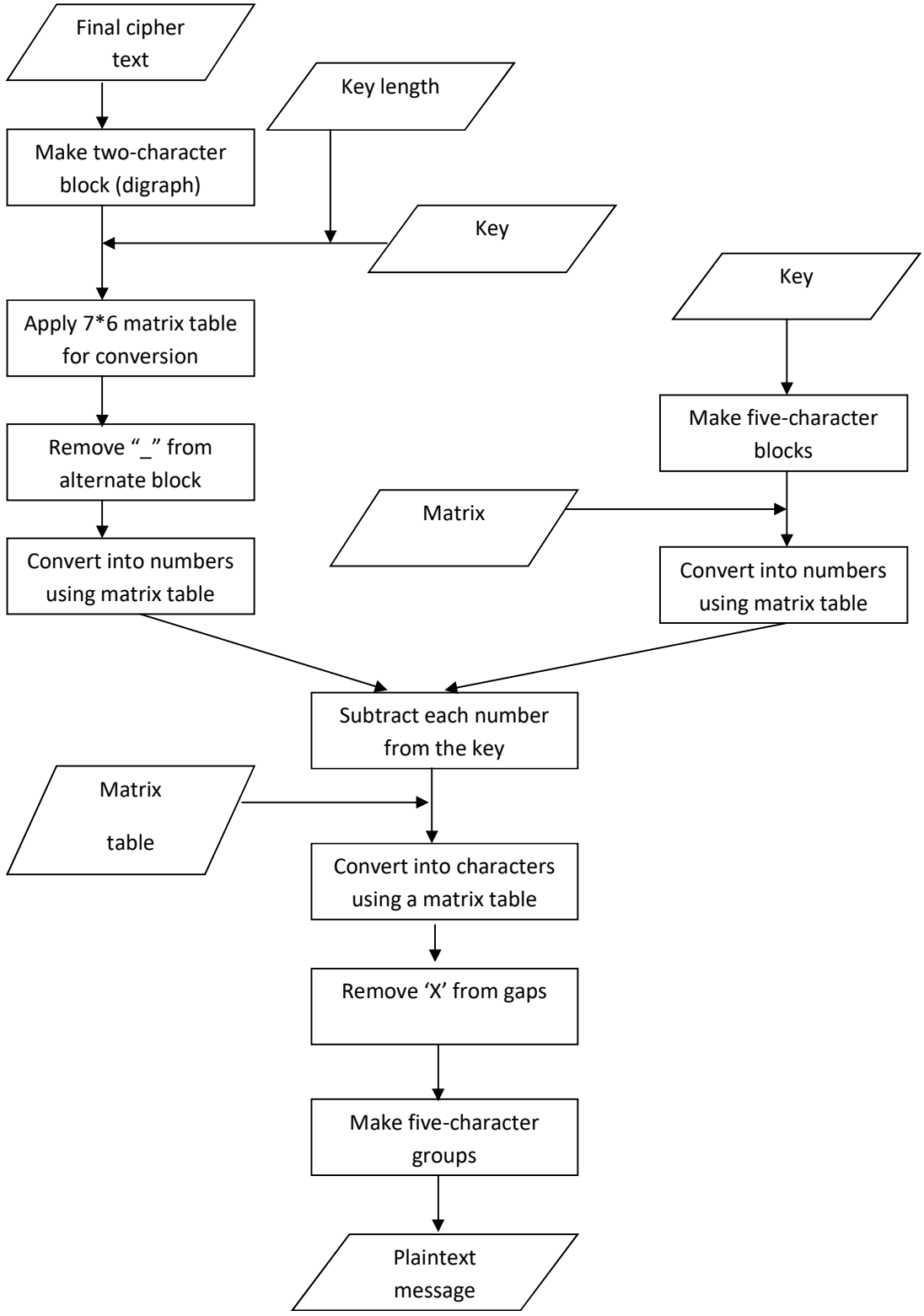


Figure 17: *HighSec* block diagram for decryption

(v) The strengths of the *HighSec* algorithm

1. The algorithm operation is easy.
   The algorithm contains seven clear steps. Every step is very clear to understand. There are no much arithmetic operations in the algorithm.

2. The algorithm is easily understandable.
   By looking at the steps, it is easy to understand what is happening to produce this algorithm.

3. It can be encrypted letters (A to Z), digits (0 to 9) and widely used symbols such as & . ?@ _
   The algorithms, normally, encrypt the letters. The HighSec proposed algorithm encrypts the letters, numbers and some widely used symbols. This will increase the usability of this algorithm.

4. The key length is dynamic; this makes the algorithm more secure.
   The key can be changed and the key length is dynamic. In this algorithm, in step 7, according to the length of key, the replacement character moves the places away up and downwards and left and rightwards. Even if someone gets the key it is not possible to decrypt the data without knowing this step (step 7). This method makes the algorithm more secure.

5. Best application for short messages and database environment.
   The databases normally contain short messages in every filed, the HighSec algorithm designed considering issues in a database environment of an organisation.

(vi) The limitations of the *HighSec* algorithm

1) The algorithm does not differentiate small from capital letters.
   This is not a weakness of an algorithm. But, making this available provides more usability. This limitation can be sorted out during the implementation process if the time permits.

2) It does not support other special symbols apart from the ones stated above.
   The other special characters are used very rarely.

3) The weak methods of transformation and protection of key and the substitution matrix table. The organisations must consider the key protection and a way to transfer the key within the organisation. Also, the matrix substitution table must be kept in a safe place. The matrix transposition table can be created using the substitution table.

(vii) The best application of the *HighSec* algorithm

The *HighSec* algorithm is very suitable for a database environment within an organisation because databases contain fields as short messages and the algorithm is developed considering the database security for short message as the key is equalised by adding characters belong from 1 according to the fixed substitution matrix table in data encryption, i.e.; E, F, G….. and so on.

In many security systems, access control and data encryption provide strong security for database environment from different kinds of attacks expected from outside or inside an organisation. The research reveals that internal attacks make more damage and it happens at a high percentage when compared to external attacks.

In this proposed high-security system, an intermediate state is added in addition to access control and data encryption for a database environment. The risks the employee connect the complete sensitive data in a database for different purposes has been cut down by the development of this added level of security.

Existing evidence firmly suggests that the proposed complete system will be capable to provide high security for databases from internal abuse of an organisation.

(viii) Validation of the HighSec algorithm

To validate the algorithm, a theoretical analysis is conducted. The theoretical analysis includes the following two key questions.

(i) Why the proposed algorithm is working (can achieve the designed goals); and
(ii) Why it is better than existing ones, and in which aspect it is better?

The HighSec algorithm is an advanced and improved version of two existing algorithms. Even though the existing techniques are traditional, they have been used for a long time

because they worked. Therefore, the improved combination of the two techniques, addressing and overcoming the weaknesses, can achieve the designed goal. The HighSec algorithm is attained through a systematic approach. The systematic approach includes the following steps:

(i) Selection of two basic cryptography algorithms - a substitution cipher and symmetric encryption techniques.
(ii) Focus on identification and analysis of weaknesses of those techniques
(iii) Addressing solutions and overcoming those weaknesses
(iv) Development of the new algorithm

While the algorithm is easy to understand and the operation includes clear steps illustrated in section 5.1.3.4 in-depth, it also encrypts letters, digits, and widely used special symbols. The length of the key is dynamic and this feature enables high security for the system. In the development of the algorithm, replacement of the characters of key moves all possible directions i.e. up, down, left and right. In that sense, even if someone gets the key it will not be possible to decrypt the message without knowing the additional step of the encryption process. This also ensures a more secure environment for the system. The EHR data includes many short messages rather than lots of notes. For example, the current MyHR system includes allergies, medications, medical history, and immunisation details rather than patient progress notes written by health care providers. Taking this into account, the development of HighSec algorithm is closely considered for a database environment with short fields of data as the key is equalised by adding characters beginning from 1 in accordance with the fixed substitution matrix table in the data encryption process, rather than starting from E, F, G and so on. Therefore, this algorithm will work very well and is more supportive of EHR environments.

Many security systems that focus on access control and data encryption mainly consider outside attacks than inside attacks. However, this security model with the HighSec algorithm discusses and focuses on internal attacks. That is why simply knowing the key will not be sufficient to decrypt the data with HighSec as discussed in section 5.1.3.4.

Some algorithms including symmetric encryption technique cannot encrypt numeric or punctuation symbols and the encrypted messages can be crashed by frequency analysis. The HighSec algorithm that has explained with the nine steps in 5.1.3.4 is new, can encrypt numeric and punctuation symbols that cannot be crashed using frequency analysis

technique. Also, some algorithms use substitution and some other use transformation. However, the HighSec algorithm uses the combination of the two methods that represent both data encryption techniques such as substitution and transformation to achieve a strong algorithm in the third level of the proposed model.

Chapter 6

Proposed Model Implementation

This chapter discusses the overall system development and implementation including the software life cycle model, system design, and system development using a computer program language, testing, and evaluation of the system. Although accordance with the scope of the project, a fully working protocol is not a requirement of this research study, the potential system development and implementation of the proposed security model are discussed and analysed to show the feasibility of the proposed method.

6.1 Software life cycle model

A software life cycle is the classification and details in which a development process phases that involve with. These phases include specification, system analysis, system designs, implementation, test, and maintenance of software. Several types of software life cycle models are available. Every software life cycle model not only describes phases of the software cycle but also the sequence in which those phases must be executed. Although the path and the order of every model differ from one to another, the basics of the models are identical. For example, generally, all software life cycle models discuss requirements, design, development or implementation and test. Every phase of any model produces at least one deliverable as the output of the phase that required for the next phase in the life cycle. For instance, the requirement analysis deliverable must be transformed into the design phase. The output of the design phase is converted for the development that includes computer programming code. The test phase verifies the deliverable of the development phase and that must be validated against the system requirements. Therefore, these phases are cycles that may occur again and again.

6.1.1 Selection of Software Life Cycle Model (SLCM)

In a prototype development, a selection of software life cycle model is one of the crucial decision-making processes. This is also based on the type of application. The waterfall model is chosen for this project. The waterfall model shows clear phases for this project to

develop a high-security model. In the waterfall model, the phases advance from one to another in a purely sequential manner. The requirements of the system should be defined clearly to continue with other phases of the model. It is also necessary to ensure the duration of every phase of the model in the early stages.

6.1.2 Rationale of the selection of the SLCM

In this project, the documentations include planning, requirement and design are comprehensively addressed and analysed in the early stages of the project before the development begins. For that reason, the waterfall model is well suited.

Also, the waterfall model is chosen for the following reasons:

1. The requirements of the system are clear and defined at early stages (i.e. during the planning of the project).
2. The phases of the proposed system are clearly defined and can be performed in a sequence manner. In other words, to perform an activity, it is important to complete the previous activity – one after another in the order.
3. The duration of the system is known at the early stages.

While the documentation is well described and available, the project with the waterfall model can easily be carried out by anyone without much interruption. In this perspective, the implementation of this project can be linked to any existing EHR system to preserve privacy and security.

The proposed privacy and security system includes three levels (phases) and every level consists of different types of protection techniques (i.e. access control, de-sensitive data access, and cryptography) to the system and a different concept is used in every level i.e. log-in pair for access control, *Pseudonymisation* for de-sensitive data access and a new algorithm for cryptography. Taking these levels, types and concept variations of privacy and security into account, the waterfall model is more appropriate as the model;

(i) defines clear stages with proper documentation and system integration,
(ii) offers a structured approach to the system that progresses linearly through discrete and
(iii) provides easily identifiable milestones in the development process.

The project is also considered as an innovative development that focuses level by level implementation with clear, concrete, and well-understood phases. This allows to build a timeline for the entire process and assign certain indicators and milestones for each level and even complete system integration. From this perspective also, the waterfall model is well-matched to this project.

As shown below in figure 18, the waterfall model covers the phases of scope definition, system plan, requirements analysis, architectural design, detailed design, coding and implementation, integration and testing, and operation and maintenance. The every phase is also discussed below.

6.1.3 Phases of the model

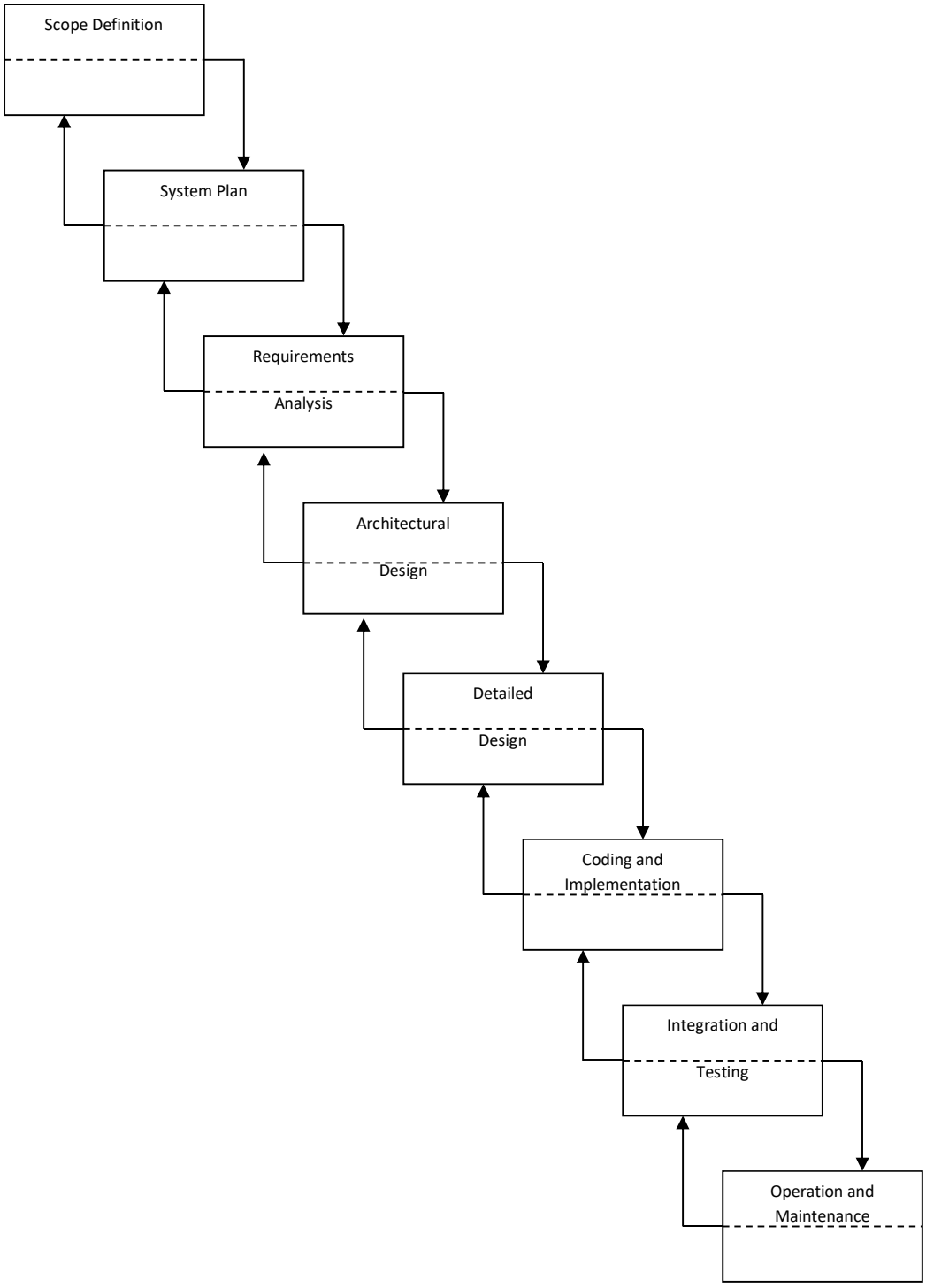


Figure 18: Phases of waterfall model for this project

6.1.3.1 Scope definition

In system development, the system scope is clearly defined and described during the planning process. The major deliverables, assumptions, and constraints are discussed in the scope statement for any system. The major deliverables are the working system and user manual documents.

6.1.3.2 System plan

The system plan is varied to a project plan that is described previously. A system is a part of a project. One of the phases of the Software Life Cycle (SLC) usually describes the plan of the system. The planning phase may include system quality, duration, and resources.

6.1.3.3 Requirement analysis

Please refer to section 6.1.4 for more details.

6.1.3.4 System design

Please refer to chapter 6.2 for system design in detail.

6.1.3.5 Coding and implementation

The coding and implementation are described separately in the report. Refer section 6.3 for coding and implementation.

6.1.3.6 Integration and testing

The part of the development of the system must be integrated to provide the expected result set. All three levels of security must be integrated into the system. Please refer to section 6.1.5 for testing.

6.1.3.7 Operation

After testing, the system is turned into an operation mode. During the system operations, system maintenance is performed. See Section 6.1.6 for system maintenance in detail.

6.1.4 Requirement Analysis

In this phase, the requirements of the proposed security system are analysed in detail. This is the process of understanding and the expectations of the proposed system. The requirement of a system is defined as a description of how a system should behave or a description of system properties or attributes. It can alternatively be a statement of *what* an application is expected to do [24].

In this protocol development, the requirement of each level of the security must be analysed one by one.

6.1.4.1 Security level 1: Login pair

Two users (a user and another super-user) must enter their username and password to enter into the system. The system design and development is explained in detail respectively in section 6.2.1 and section 6.3.2.

6.1.4.2 Security level 2: An intermediate state of the database

The sensitive data of the database is hidden and users can access only alternate data for the specific view that will be able to work with to complete their employee role. The views can be defined through the user privileges. Please refer to section 6.2.2 and section 6.3.3 for further details to design and development.

6.1.4.3 Security level 3: Cryptography / data encryption and decryption

A new algorithm for encryption and decryption is proposed and developed to perform data encryption before store data into database and data decryption before downloading the data from the database. Please refer to section 6.2.3 and section 6.3.2 for further details on the design and development of the concept.

6.1.5 Test cases and testing

A test case is a set of conditions of variables to assist in performing a test of the system functionalities. The test will be performed according to the requirements that are identified in section 6.1.4 to perform a thorough test to validate whether all the requirements of the application are met. There must be at least one test case for each requirement. In this proposed security system, the test is performed based on security levels.

6.1.5.1 Security level 1: Login pair

The test cases are created and tested to ensure the following activities in level one.

(i) A user can't be the pair user

(ii) Any other user can't be the pair user except the allocated pair

(iii) The selected manager can be login instead of any pair super-user

(iv) A user can change his/her password at any time.

6.1.5.2 Security level 2: An intermediate state of the database

The test cases are created and tested to ensure the following activities in level two.

(i) The health sensitive data must create a reference number to represent before save it to tables.

(ii) The reference number only can be viewed for sensitive data when access.

(iii) The administrator only can view sensitive data when required.

6.1.5.3 Security level 3: Cryptography / data encryption

The test cases are created and tested to ensure the following activities in level three.

(i) The data is encrypted before it is saved or stored into the database

(ii) The data is decrypted when a request is made to download before accessing it.

6.1.6 System operation and maintenance

The system is in operation mode after testing it. There may be ongoing changes and requires the need for further development or modification in any system. In reality, it is very difficult to identify and include all aspects of the system entirely in the development and implementation process. Additional requirements or changes arise from time to time and they need to be resolved; hence, this process is referred to as maintenance. In this model, three levels of security are considered.

6.1.6.1 Security level 1: Login pair

It is logically created and put in the development. It is not known, practically, how effective for security in an organisation. When this level comes to operation it might be modified to meet the actual requirements.

6.1.6.2 Security level 2: An intermediate state of the database

In viewing intermediate alternate data for users is a secure and safe way to protect data but it is not known how effective nor how it satisfies the needs of the users in an organisation setting.

6.1.6.3 Security level 3: Cryptography / data encryption

In an operation environment, the new algorithm would be useful for the data encryption and decryption functions for the database environment.

6.2 System Design

This security system has three tires with each tier having a different type of security method. Hence, the proposed complete system in this design provides security against different types of threats which can be expected from the diverse sources.

6.2.1 Level 1 design: Access Control: *Log-in Pair*

As the first step in this process, employees must be paired. For example, six employees in an organisation need access to the system then they will be grouped into three pairs. During the process of pairing, the following main factors (criteria) need to be considered;

(i) It will be easy if the employees who are physically located (e.g.; shares the same room) close to each other to be made as a pair.

(ii) It will be beneficial for the organisation if the employees who are more involved with direct access to the system are paired together. For example, identifying and grouping a user and a super-user that access the same kind of health information for the same purpose can be paired together.

(iii) It is also useful if the number of times (or hours) an employee needs to work within the system is also considered in the pairing. For instance, a user who needs to use the system for the whole day, all seven days a week should be paired with another super-user who also uses the system for the long-time of the period rather than with a super-user who need to access the system only for few hours in a week.

Also, the guidance of administration must be prioritised when performing the design of the pairing process. The pair design for users (considering six users A, B, C, D, E & F) in an organisation can be paired or grouped as described below in table 17.

Table 17: The revised design phase of log-in pair

Pair	Staff
1	A or X or Y & B or X or Y
2	C or X or Y & D or X or Y
3	E or X or Y & F or X or Y

The detail design of the model in level one is illustrated below in figure 19. As discussed previously the log-in page for the level one includes both the user and super-user credential input interface and the option for super-users to change their username and password when required. The ability to change their credentials anytime for super-users also increases the privacy and security of the system.

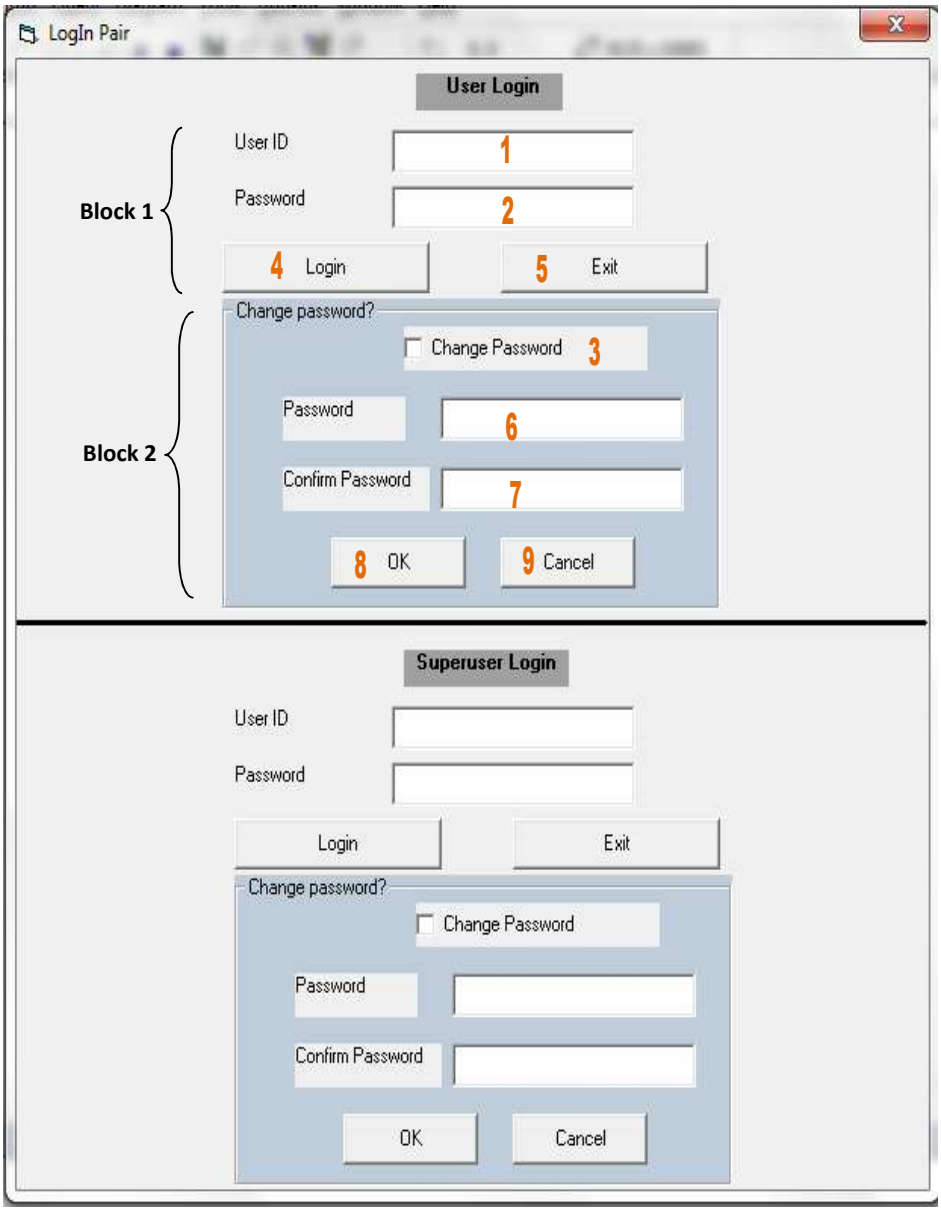


Figure 19: Designing log-in pair interface

The specification:

1) *Item – text box. Input into user_pw.u_id.*
2) *Item – text box. Input into user_pw.u_pw*
3) *Item - check box. Value (Y/N). If Value = 'Y' open Block 2 and enable. If value ='N' hide Block 2.*
4) *Item - push button. On press open the main form.*
5) *Item – push button. On press exit from the application*
6) *Item – text box. Input into Block2.new_password.*
7) *Item – text box. Input into Block2.confirm_password.*
8) *Item - push button.*
   On press check that, if (New password = confirm password)
   alter table user_pw
   setu_pw = new_password;
   commit change.
9) *Item - push button. On press clear item new_password, confirm_password. Hide block 2.*

6.2.2 Level 2 design: An Intermediate State of Database (ISD)

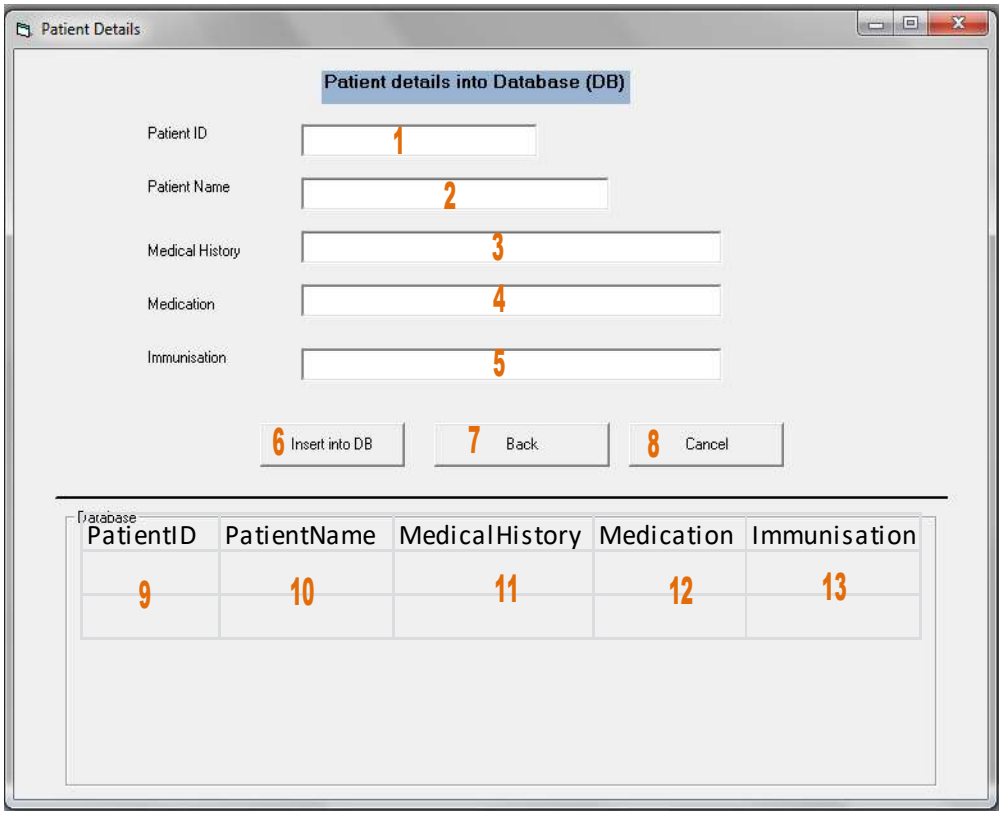


Figure 20: Designing ISD interface

Once all the details are entered onto all the textboxes in the above figure 20, the push button called *Insert into DB* should be clicked to save the information into the database. At this point, the *pseudonymisation* technique will start to work by replacing the sensitive information in the database with meaningless information. The saved information can be viewed at the *Display Database Table*.

The step when click button *Insert into DB* the connective table with valid information will be saved in a different location as shown in figure 21 as an example.

Patient Account

Patient Account Number	Patient ID
12345678	1
53478865	235
97643322	2340

Patient Name	Patient Name ID
John Wales	7
Smith Paul	23
Vimal	1097

Figure 21: Designing ISD hidden concept

When it is required, the connective table will be accessed to retrieve the original health sensitive data from the database.

The specification:

1) *Item – text box. Input into pati_acc_no.*
2) *Item – text box. Input into pati_name*
3) *Item – text box. Input pati_history*
4) *Item – text box. Input pati_medication.*
5) *Item – text box. Input pati_immunisation*
6) *Item – push button. On press save item 1, 2, 3, 4, & 5.*
7) *Item – push button. On press go previous page.*

8) *Item - push button. On press clear item 1,2,3,4 & 5*
In display database table:
9) *Item – column pati_id.*
10) *Item – column pati_name_id*
11) *Item – column pati_history*
12) *Item – column pati_medication*
13) *Item – column pati_imminisation*

6.2.3 Level-3 design: Cryptography / Data Encryption

In a practice setting, once a patient account number (that is created when a patient registers with the health care provider organisation), the patient name, past history, current medication, and immunisation details are given, the sensitive information can be encrypted using the encryption key. Similarly, the information can be decrypted using the decryption key to view/access the information. This process of the interface is shown below in figure 22.

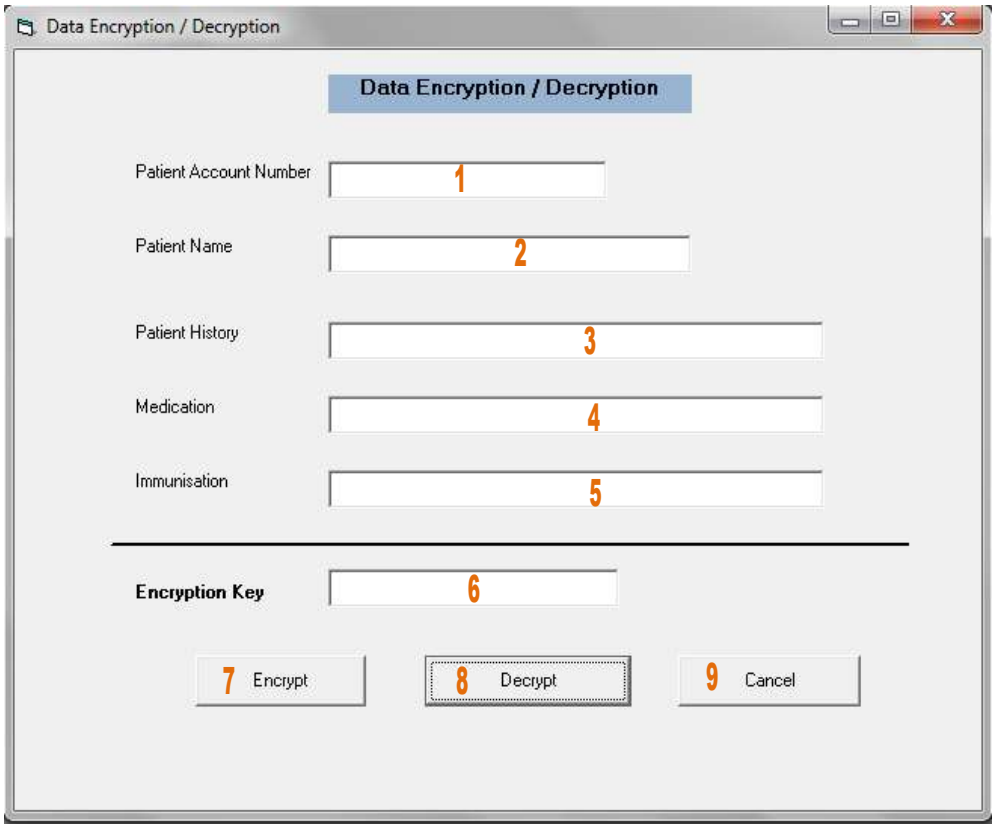


Figure 22: Designing data encryption and decryption interface

The specification:

1) *Item – text box. Input into pati_acc_no.*
2) *Item – text box. Input into pati_name*
3) *Item – text box. Input pati_history*
4) *Item – text box. Input pati_medication.*
5) *Item – text box. Input patient_immunisation*
6) *Item – text box. Input encry_key*
7) *Item – push button. On press do encryption & save item 1, 2, 3, 4, & 5.*
8) *Item – push button. On press do decryption & save item 1,2,3,4 & 5.*
9) *Item - push button. On press clear item 1,2,3,4, 5 & 6.*

When the button *Encrypt* is clicked after every textbox field and key are completed, the encryption process will be performed according to the new strong algorithm that is explained in chapter 5. The encrypted data will be stored permanently in the database for future accesses.

6.2.4 Complete system design and integration

The security model is described as a three-tier concept. Even though, every tier of the model addresses different security technique and threat, the tiers must be brought together as a whole system to achieve the objectives of the model. Table 18 explicates the type of security, the unique concept used, and the level of protection every tier provides.

Table 18: Complete system design and integration

Security level	Security type	Unique concept	Protection type
One	Access control	Log-in pair	Basic entry into the system
Two	De-sensitive data access	Pseudonymisation	Intermediate data access
Three	Cryptography / data encryption and decryption	Strong new algorithm	Full data access

Figure 23 describes the complete system as a whole. Although the system is described with three levels, the levels do not have a necessity to work in sequence. For example, levels one and two can work together for some type of users and levels one and three work together for another. It is based on what information the users trying to access and its sensitivity.

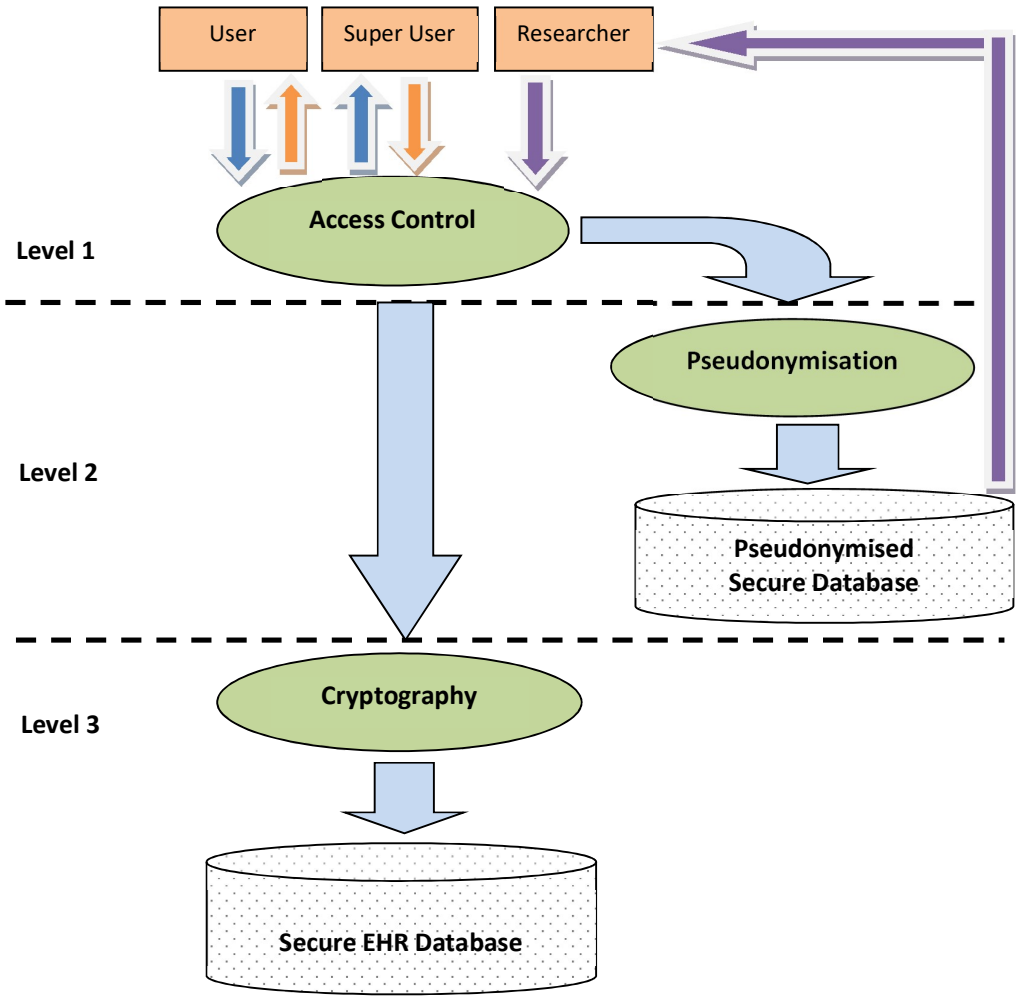


Figure 23: Complete *HighSec* system architecture design

6.3 System Implementation

The system implementation discusses how system design can convert into a working protocol. Based on the system design, the protocol is divided into modules or units and every unit will be described in computer program codes. In other words, the entire system needs to be separated as a small program unit. In the system implementation phase, the design must be decoded into a machine-readable form. If the design of a software product is completed in detail, generating code for the design can be accomplished without any

difficulties. A wide range of high-level computer programming languages is currently available for the coding phase. The selection of an appropriate programming language for a specific project is also another decision-making. For example, if an inappropriate language is chosen, it would be difficult to include all the features of the project. In some other cases, the use- friendliness of the end-user system may be affected when this decision is incorrectly made.

Each level of the proposed *HighSec* security system considered as a unit and the implementation performed in this phase. There are three units for the implementation in this proposed system.

Unit 1 – security level 1: *login pair*

Unit 2 – security level 2: *ISD*

Unit 3 – security level 3: *Cryptography / data encryption and decry*ption

6.3.1 Selection of the right programming language

Visual Basic 6 is chosen as the appropriate programming language to implement the proposed *HighSec* security system.

To choose the right programming language the following factors are considered.

(i) Type of application

The *HighSec* is a security-based application to handle data in a safe method.

(ii) The complexity of the system

The complexity of the *HighSec* security system is expected at a medium level based on the fact that the system must work with the right balance between accessibility and security.

(iii) Developer knowledge / experience

The author is the developer of this project at this stage. The knowledge and experiences of the author also need to be considered to resolve upcoming issues related to the system's maintenance.

(iv) Visualisation and user-friendliness

It is also necessary to visualise the system graphically to understand it well and increase the user-friendliness.

6.3.2 System Coding

As previously stated, to develop any software system, the detail designing phase has to be converted into a machine-understandable language using any programs. The programming language is chosen based on the type of system application and other related factors. To develop the *HighSec* security system, *Visual Basic.6* programming language is used. The main coding of the system is described below in section 6.3.2.1.

6.3.2.1 Coding for level-1 security: Login pair

The coding for the login pair concept is also discussed previously in one of the Author's research papers [78, 131 – Author's previous publications].

```
Function checkdata() As Boolean
bcheck = True
   If txtuser.Text = "" Then
MsgBox "Enter user name", , "HighSec System"
txtuser.SetFocus
bcheck = False
       Exit Function
   End If
   If txtpassword.Text = "" Then
MsgBox "Enter Password", , "HighSec System"
txtpassword.SetFocus
bcheck = False
       Exit Function
   End If
    If cmbUsertype.Text = "Normal" Then
       If cmbManager.Text = "Select" Then
MsgBox "Select Manager", , "HighSec System"
txtpassword.SetFocus
bcheck = False
          Exit Function
       End If
    End If
checkdata = bcheck
End Function

Private Sub cmbUsertype_Click()
   If cmbUsertype.Text = "Normal" Then
      Frame1.Visible = True
   Else
      Frame1.Visible = False
   End If
End Sub

Private Sub cmdExit_Click()
   Unload Me
End Sub

Private Sub cmdok_Click()
bcheck = checkdata
usertype = Left(cmbUsertype.Text, 1)
 If bcheck = checkdata Then
rs.Open "select * from usertable where userid='" + txtuser.Text + "'", cn
       If Not rs.EOF And Not rs.BOFThen
MsgBox "This user already exists", , "HighSec System"
       Else
newpwd = encryptdata(txtpassword.Text, newkey)
newpwd = txtpassword.Text
ssql = "insert into usertable (userid,pwd,usertype) values('" + txtuser.Text + "','" + newpwd + "','" +
usertype + "')"
InputBox "", ,ssql
```

```
cn.Executessql
        If usertype = "N" Then
ssql = "insert into groupuser (user1,user2) values('" + txtuser.Text + "','" + cmbManager.Text + "')"
cn.Executessql
        End If
ans = MsgBox("User created succesfully. " + vbCrLf + " Do you want to close this window?",
vbYesNo)
        If ans = vbYes Then
            Unload Me
        Else
txtuser.Text = ""
txtpassword.Text = ""
        End If
      End If
rs.Close
   End If
End Sub

Private Sub Form_Load()
ssql = "select * from usertable where usertype='M'"
rs.Openssql, cn
While Notrs.EOF
cmbManager.AddItemrs(0)
rs.MoveNext
Wend
rs.Close
cmbUsertype.ListIndex = 0
End Sub
```

6.3.2.2 Coding for level-2 security: ISD

In this level, there is no specific coding developed to implement the ISD. This level of the *HighSec* security system is described with the database creation. However, it has been suggested for further development in section 7.2.

6.3.2.3 Coding for level-3 security: Cryptography

```
Sub Main()
cn.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" + App.Path + "\userdb.mdb;Persist Security
Info=False"
firstlogin = True
' key = "AIM"
   j = 1

   For i = 69 To 69 + 21
arrTab(j) = Chr(i)
      j = j + 1

   Next
   For i = 0 To 9
arrTab(j) = CStr(i)
      j = j + 1

   Next
arrTab(j) = "_"
   j = j + 1

arrTab(j) = "?"
   j = j + 1

arrTab(j) = "@"
   j = j + 1

arrTab(j) = ","
   j = j + 1

arrTab(j) = "."
   j = j + 1
```

```
arrTab(j) = "&"
   j = j + 1

   For i = 65 To 65 + 3
arrTab(j) = Chr(i)
      j = j + 1

   Next
'  frmmenu.Show
'  frmuser.Show
   'frmcustomer.Show
   Form1.Show
End Sub

Public Function encryptdata(plaintext As String, key As String) As String

Dim lenkey, lenplain
Dim cipher As String, newkey As String
lenkey = Len(key)
'lenplain = Len(plaintext)
k = 1
newkey = key
For i = Len(key) + 1 To Len(plaintext)
newkey = newkey&arrTab(k)
   k = k + 1
Next

lenplain = Len(plaintext)
For i = 1 To Len(plaintext)
   For j = 1 To 42
plainchar = Mid(plaintext, i, 1)
      If plainchar = arrTab(j) Then
foundchar = True
plainno = j
         Exit For
      End If
   Next
   If foundchar Then
foundchar = False
      For j = 1 To 42
plainchar = Mid(newkey, i, 1)
         If plainchar = arrTab(j) Then
keyno = j
foundchar = True
            Exit For
         End If
      Next
   End If
   If foundchar Then
      NO = (plainno + keyno) Mod 43
cipher = cipher &arrTab(NO)
   Else
      cipher = ""
      Exit For
   End If
Next
encryptdata = cipher

End Function
Public Function decryptdata(ciphertext As String, key As String) As String
Dim lenkey, lenplain
Dim cipher As String, newkey As String
lenkey = Len(key)
k = 1
newkey = key
For i = Len(key) + 1 To Len(ciphertext)
newkey = newkey&arrTab(k)
   k = k + 1
Next

lenplain = Len(ciphertext)
For i = 1 To Len(ciphertext)
   For j = 1 To 42
plainchar = Mid(ciphertext, i, 1)
      If plainchar = arrTab(j) Then
```

```
foundchar =
True

plainno = j
          Exit For
       End If
    Next
    If foundchar Then
foundchar = False
       For j = 1 To 42
plainchar = Mid(newkey, i, 1)
          If plainchar = arrTab(j) Then
keyno = j
foundchar = True
             Exit For
          End If
       Next
    End If
    If foundchar Then
       NO = plainno - keyno

       If NO < 0 Then
          NO = NO + 43
ElseIf NO = 0 Then
          NO = NO + 42
       End If

plaintext = plaintext &arrTab(NO)
    Else
       plaintext = ""
       Exit For
    End If
Next


decryptdata = plaintext
End Function
Public Function getpositioninmatrix(char1 As String, pos() As Integer)
found = False
    For i = 1 To 6
       For j = 1 To 7
          If char1 = playmat(i, j) Then
pos(1) = i
pos(2) = j
found = True
             Exit For
          End If
       Next
       If found Then
          Exit For
       End If
    Next

End Function
Public Function getcharfor(ro As Integer, col As Integer, ro1 As Integer, col1 As Integer, cipherchar() As String)

    If ro<> ro1 And col <> col1 Then
cipherchar(1) = playmat(ro, col1)
cipherchar(2) = playmat(ro1, col)
ElseIfro = ro1 Then
colpos = (col + keylength) Mod 7
       If colpos = 0 Then
colpos = 1
       End If
cipherchar(1) = playmat(ro, colpos)
colpos = (col1 + keylength) Mod 7
       If colpos = 0 Then
colpos = 1
       End If
cipherchar(2) = playmat(ro1, colpos)

ElseIf col = col1 Then
ropos = (ro + keylength) Mod 6
       If ropos = 0 Then
ropos = 1
       End If
```

```
cipherchar(1) = playmat(ropos, col)
ropos = (ro1 + keylength) Mod 6
        If ropos = 0 Then
ropos = 1
       End If
cipherchar(2) = playmat(ropos, col1)
   End If
getcharfor = cipherchar
End Function
Public Function getdecharfor(ro As Integer, col As Integer, ro1 As Integer, col1 As Integer, decipherchar() As
String)
   If ro<> ro1 And col <> col1 Then
decipherchar(1) = playmat(ro, col1)
decipherchar(2) = playmat(ro1, col)
ElseIfro = ro1 Then
colpos = col - keylength
       If colpos<= 0 Then
colpos = colpos + 7
       End If
       'colpos = col - (keylength Mod 7)
decipherchar(1) = playmat(ro, colpos)
       'colpos = col1 - (keylength Mod 7)
colpos = col1 - keylength
       If colpos<= 0 Then
colpos = colpos + 7
       End If
decipherchar(2) = playmat(ro1, colpos)
ElseIf col = col1 Then
       'ropos = (ro - keylength Mod 6)
ropos = ro - keylength
       If ropos<= 0 Then
ropos = ropos + 6
       End If
decipherchar(1) = playmat(ropos, col)
' ropos = (ro1 - keylength Mod 6)
ropos = ro1 - keylength
       If ropos<= 0 Then
ropos = ropos + 6
       End If
decipherchar(2) = playmat(ropos, col1)
   End If
getdecharfor = cipherchar
End Function
Public Function decryptPlay(ciphertext As String) As String
   Dim char1 As String, char2 As String
   Dim pos1(2) As Integer
   Dim pos2(2) As Integer
   Dim cipherplay(2) As String
prevchar = ""
strtext = ""
   For i = 1 To Len(ciphertext) Step 2
       char1 = Mid(ciphertext, i, 1)
       char2 = Mid(ciphertext, i + 1, 1)
getpositioninmatrix char1, pos1
getpositioninmatrix char2, pos2

getdecharfor pos1(1), pos1(2), pos2(1), pos2(2), cipherplay
playcipher = playcipher&cipherplay(1) &cipherplay(2)
   Next
'    Form1.Text6.text = playcipher
   For i = 1 To Len(playcipher)
       char1 = Mid(playcipher, i, 1)
       If char1 <> "_" Then
playdecipher = playdecipher& char1
       End If
   Next
   'If Len(playtext) Mod 2 <> 0 Then
   '    playtext = playtext& "X"
   'End If
decryptPlay = playdecipher
End Function
Public Function encryptPlay(plaintext As String) As String
   Dim char1 As String, char2 As String
   Dim pos1(2) As Integer
   Dim pos2(2) As Integer
   Dim cipherplay(2) As String
```

```
prevchar = ""
strtext = ""
    Dim playcipher As String, playtext As String
    For i = 1 To Len(plaintext)
        char1 = Mid(plaintext, i, 1)
        char2 = Mid(plaintext, i + 1, 1)
        If char1 = char2 Then
playtext = playtext& char1
playtext = playtext& "_"
        Else
playtext = playtext& char1
playtext = playtext& char2
i = i + 1
        End If
    Next
    If Len(playtext) Mod 2 <> 0 Then
playtext = playtext& "X"
    End If
'    Form1.Text5.Text = playtext
    For i = 1 To Len(playtext) Step 2
        char1 = Mid(playtext, i, 1)
        char2 = Mid(playtext, i + 1, 1)
getpositioninmatrix char1, pos1
getpositioninmatrix char2, pos2

getcharfor pos1(1), pos1(2), pos2(1), pos2(2), cipherplay
playcipher = playcipher + cipherplay(1) + cipherplay(2)
    Next
encryptPlay = playcipher
End Function

Function createPlayTable(strkey As String)
    Dim playchar As String
lenkey = Len(strkey)
    Dim playtabchar As String
    k = 1
     For i = 1 To 6
        For j = 1 To 7
playmat(i, j) = ""
playarr(k) = ""
            k = k + 1
        Next
    Next
    k = 1
    For i = 1 To 6
        For j = 1 To 7
            If (k <= lenkey) Then
playchar = Mid(strkey, k, 1)
            Else
                For m = 1 To 42
bfound = False
                    For l = 1 To k
                        If arrTab(m) = playarr(l) Then
bfound = True
                            Exit For
                        End If
                    Next
                    If Not bfoundThen
playchar = arrTab(m)
                        Exit For
                    End If
                Next

            End If
playtabchar = playtabchar&playchar
playmat(i, j) = playchar
playarr(k) = playchar
            k = k + 1
        Next
    Next
' MsgBoxplaytabchar
End Function

Function encrypt(txt As String, mykey As String)
    Dim txt1 As String, txt2 As String
    txt1 = encryptdata(txt, mykey)
```

```
createPlayTable (mykey)
keylength = Len(mykey)
   txt2 = encryptPlay(txt1)
   'txt2 = txt1
encrypt = txt2
End Function

Function decrypt(txt As String, mykey As String)
   Dim txt1 As String, txt2 As String
createPlayTable (mykey)
keylength = Len(mykey)
   txt2 = decryptPlay(txt)
' txt2 = txt
   txt1 = decryptdata(txt2, mykey)

decrypt = txt1
End Function
```

6.4 System testing and evaluation

In this section, the different issues addressed by the research and system are reviewed and evaluated. It is evident that the project research has been undertaken in the right way and the developed system functions well. Also, the evaluation itself provides a guarantee for the overall project and its quality.

6.4.1 Evaluation of the research methodology

The research has been undertaken to prove the followings;

(i) Any information system can be attacked by threats.

(ii) Databases are more vulnerable to get attacked.

(iii) Internal abuses are the main reason for database attacks than external database attacks.

(iv) An access control mechanism provides a level of security.

(v) An intermediate state of the database (ISD) provides a level of security.

(vi) An ISD also prevents internal abuses.

(vii) Data encryption provides a level of security.

(viii) All three layers/ tiers/ levels provide overall security for the *HighSec* system.

Table 19 describes the evaluation of the research methodology that provided above. In the description, every evaluation/review item verifies whether the proposed method functions for the specific evaluation item and the reference where the details of the evaluation process can be found.

Table 19: Evaluation of the research methodology

	Evaluation / Review	Definition	Reference
1	Can any information system be attacked by threats?	Yes. No system is 100% fully secure in the world. There are several different attacks recorded and revealed in the past. Every attack is formed a different type, they are caused differently and the impact of the attack also varies.	Section 2.7.1, 2.7.2 and 4.1
2	Are databases more vulnerable to attack?	Yes. Databases are stored in storage devices permanently and the data stored are normally, in plaintext. So the abuses and attacks are always possible and increase the possibility of the attack.	Section 2.7
3	Are internal abuses the main reasons in database attack than external abuses?	Yes. The past researches have revealed that internal abuse is the main challenge for database security in an organisation.	Section 2.7 and 4.1
4	Does the access control mechanism provide a level of security?	Yes. The access control mechanism (login with user ID and password) provides basic initial security for the system	Section 2.5 and 2.6
5	Does an intermediate state of the database (ISD) provide a level of security?	Yes. Accessing hidden format with relations for sensitive data increases the security and usability of the system.	Section 3.3.2, 4.3.2 and 5.1.2
6	Does ISD prevent internal abuses?	Yes. Daily users of the system access only ISD and they cannot abuse the data in those settings.	Section 6.2.2, 6.3.2 and 6.4.3
7	Does data encryption provide a level of security?	Yes. After encrypting data it is useless to be attacked or abused. Without knowing the way to decrypt using the correct key, the data is protected and this provides a level of security.	Section 6.2.3, 6.4.4
8	Are all three levels of the model provides overall security for the *HighSec* system?	Yes. The proposed *HighSec* system is developed from the result and the findings of the research undertaken. Overall, it covers different forms of attack from different sources. Therefore, the *HighSec* system can be recommended for the MyHRs to provide the overall security of the system.	Chapter 6.1, 6.2, 6.3 and 6.4

6.4.2 Evaluation of the level 1 security: log-in pair

The level one security is a basic access control function. However, it is an improved version because of the login pair concept. The following results are expected from the requirements and design of the system:

(i) A user cannot be the super-user

(ii) Any other user cannot be the super-user except the allocated pair

(iii) A selected manager can log in instead of any super-user if necessary

(iv) Any user or super-user can change his/her password at any time.

The evaluation process of the level one is illustrated below in table 20.

Table 20: Evaluation of the level one security: log-in pair

	Evaluation / Review	Definition	Reference
1	A user cannot be the super-user?	Any user of the system needs a super-user permission to enter into the system. If a user provides the same username and password for super-user fields as well, the system will not allow the user to enter in.	Section 5.1.1, 6.2.1 and 6.3.1
2	Any other user cannot be the super-user except the allocated pair?	Yes. The allocated pair user only will be allowed for particular user access. If any other combination with the username and password cannot be accepted and the system displays the message that the super-user is unauthorised.	Section 5.1.1, 6.2.1 and 6.3.1
3	Does a selected manager can login instead of any super-user?	Yes. This is the solution suggested for the absence of any super-user. A selected manager can log in for any user when the super-user is in absence at work.	Section 5.1.1, 6.2.1 and 6.3.1
4	Can any user change his/ her password any time?	Yes. There is an additional option that permits users and super-users to change the password at any time. This ability of a user provides more privacy and security of the system.	Section 6.2.1

6.4.3 Evaluation of the level two security: ISD

The second level of the security model provides additional security by hiding the sensitive data and showing only the reference number or pseudonyms to the user. Creating the

reference number or pseudonyms for sensitive data is evaluated. However, getting the reference number or pseudonyms to display to the user and retrieving it whenever required options need to be developed in further development**.**

6.4.4 Evaluation of the level three security: cryptography/ data encryption

This evaluation process is also discussed in one of the author's research papers [79 - Author's previous publication]. The third level of the *HighSec* security model is data encryption and data decryption. This level of security is expected to do the followings:

(i) Data are encrypted before saving or storing it into the database.

(ii) Data are decrypted when the data is requested to download.

The evaluation process of the level three (cryptography – data encryption/decryption) is discussed in table 21.

Table 21: Evaluation of the level three security: cryptography/data encryption

	Evaluation / Review	Definition	Reference
1	Are data encrypted before saving into the database?	Yes. Using the *HighSec* new algorithm, the encryption is done before saving into the databases.	Section 6.2.3
2	Are data decrypted when required?	Yes. Using the *HighSec* new algorithm, the decryption is done before retrieving the date from databases.	Section 6.4.3

Chapter 7

Conclusions and Future Work

7.1 Conclusions

At the outset of the proposed model, various aspects are discussed. Information Technology (IT) shows rapid improvement in health care in the last two decades. It seems that the world cannot function without IT. However, any advancement carries some inherent problems with it. In the case of IT, information privacy and security could be considered as one of the major problems. With the invention and rapid growth of eHealth systems including MyHRs, the information privacy, and security issues become very significant.

Throughout this thesis, to build a clear understanding of the privacy and security issues associated with storing and accessing MyHR systems' that deal with sensitive health information is discussed comprehensively. It is started by taking a look at health information security, health database security and potential internal abuses in a health care provider organisation setting in the big picture of information security is in a broader concept. It has also reviewed recent researches and concluded that internal abuse plays the main role than external attack in health information security.

The different health care database attacks and the potential solutions for those attacks have been analysed to achieve a high-security system. The three-tier architecture was designed and developed as a proposed system. The three-tiers are access control, an intermediate state of database and cryptography (data encryption and decryption). The justifications are given why these three architectures are designed, how these tiers cover the different forms of attacks, and how the whole system works together to confirm the security for a health care environment. Besides, each tier is analysed to improve the security itself. The *login pair* concept is a specialised improved version of the access control concept.

The proposed three-tier architecture is illustrated well. A new data encryption algorithm has been designed for the third tier of the system. To design this new algorithm, two

existing algorithms are analysed. The weaknesses of those existing algorithms have been overcome in the new method. To increase the accessibility and usability of the MyHR system, *pseudonymisation* technique is used in the second tier.

To develop the proposed system, a suitable software life cycle model is selected and the phases of the model are developed to prove the functionality of the system. The developed system tested and evaluated against the expected outcome of every tier. Although delivering a working protocol security system is not the outcome of this research, the potential system development process and the feasibility of it are explicated. Collectively, the three-tier model framework is discussed and proved that the system will provide high security for any EHR systems including the MyHR. This development will assist to build confidence and trust with the MyHRs.

The privacy and security issues can be mitigated or prevented by putting in appropriate security mechanisms. Having mentioned that, it is very difficult to prevent those issues completely. While keeping this in mind, the benefits of the MyHR need to be weighed against those concerns. The assessment ends up with better health care versus privacy and security concerns. However, privacy and security is not the only issue to overcome the concerns of the MyHR usage. Also, data integrity and system compatibility are two of many. Strictly using an international standard medical terminology without free text options for medical history and medications may be a solution to reduce the concerns related to data integrity. To decrease the concerns of system compatibility, the software vendors must be given clear identical requirements and specifications to develop the integration to the MyHR that every software vendor must follow to continue their business in the sector.

Finally, accessibility is the key to any EHR system including MyHR. However, to preserve the privacy and security of the system, the application of appropriate security controls are required. These security controls directly impact the accessibility of the system. Therefore, the right balance of security controls and accessibility is very important to ensure the usage of MyHR system.

7.2 Future Work

The security level one discusses an advanced access control mechanism known as l*ogin pair*. This is an improved version of the access control method. However, this initiative requires some additional considerations when designing the pairs. The considerations and factors are discussed in section 6.2.1. Furthermore, in this concept, any breaches together from both users and super-users cannot be identified and resolved. To determine these circumstances, a system monitor facility that will detect the user activities during the access to MyHR would be beneficial to increase the level of security of the system. Hence, the System Monitoring Facility (SMF) can be suggested for further development in level one. Also, from the privacy and security perspective, in this project, a mobile security system is discussed for the communication between user and super-user. More research may be required to understand the efficiency of the system in the process of;

(i) User request being sent to super-user
(ii) Ensuring the super-user responds or unavailable to respond within a time frame
(iii) The message of approval, refusal, or unavailability being sent back to the user within a time frame.

The level two that outlines the ISD will preserve privacy and security by sharing sensitive data within and /or outside of a health care provider organisation. This concept offers a role-based view according to the staff members' job requirements. The national health services utilise this concept to preserve the patients' privacy in England. This level of security will preserve the privacy and security of the system while increasing the accessibility by offering *pseudonyms* and the data relationships for users. Therefore, further development may be required to create *pseudonyms* for sensitive health information in the MyHR.

The level three is cryptography that describes a new algorithm for encryption and decryption. This level shows an improved version of two existing algorithms. Further development can fine-tune the system, for example, differentiating uppercase from lowercase. Also, any technical and practical issues that be identified in the system operation stage can be suggested for further development in the maintenance phase.

Additionally, further research and discussion is required on how the patients' concerns of privacy, confidentiality, and security impact the health outcome in Australian communities.

While the patients are willing to travel outside of their community to preserve the privacy of their health, these concerns directly interrupt their health care. The patients' level of trust in their health care providers and their security controls need to be improved. Therefore, the health care providers need to prove that they have appropriate security mechanisms, policies and framework in place to preserve the privacy of sensitive health information. Incidents of failing to preserve privacy and any breaches affect their business.

Further community-based research is also necessary to understand how the MyHR influences at the local community level. The government encourages the adoption of health care providers' to the system and focuses on numbers of registration rather than emphases on communities. A community is a smaller unit of a nation. On this basis, all health care providers in a community must be connected to MyHR and trial the system to understand the real-world impact on the new initiative in Australia. This community-based learning and findings from the research would be beneficial when developing the nation-wide EHR system like MyHR. Given the fact that it is difficult to prevent the privacy and security concerns completely of any EHR systems, the system itself should be able to reveal the benefits of using it rather than the fears of privacy and security. The benefits need to be identified and prioritised on top than the concerns and this will encourage the patients to use the system more. Therefore, in addition to develop security controls to build patients' trust, this kind of research will assist to prove to patients how the new system impacts positively in their day to day health-life and contributes to deliver better health care for them.

Reference

[1] Pearce, C. (2009). Electronic medical records - where to from here?, Professional Practice, Melbourne.

[2] McInnes, D. K., Slatman, D. C., & Kidd, M. R. (2011). General practitioners' use of computers for prescribing and electronic health records: results from a national survey, Australia. [online] Available at: <http://www.clinfowiki.org /wiki/index.php/ General_practitioners%27_use_of_computers_for_prescribing_ and_ electronic_ health_ records: _results_ from_ a_ national_ survey>. [Accessed 12 March 2016].

[3] Iakovidis, I. (1998). Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Health care Records in Europe. International Journal of Medical Informatics vol. 52 no. 128, pp. 105 –117.

[4] Shekelle, P., Morton, S. C., & Keeler, E. B. (2006). Costs and Benefits of Health Information Technology. Evidence Reports/Technology Assessments, No. 132. National Institutes of Health, NJ.

[5] Rash, M. C. (2005). Privacy concerns hinder electronic medical records, The Business Journal of the Greater Triad Area. BIZjournals, NC.

[6] Choe, J., & Yoo, S. K. (2008). Web-based secure access from multiple patient repositories. Inetrnational Journal Of Medical Informatics, 77 (4), 242-248.

[7] Office of the Australian Information Commissioner APP8 (2015). Cross-border Disclosure of Personal Information and for more information, see the Office of the Australian Information Commissioner. [online] Available at: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information> [Accessed 02 February 2019].

[8] Funnell, A. (2016). Your Health Information is Neither Safe Nor Secure. ABC News. [online] Available at: <abc.net.au/news/2016-11-12/your-health-information-is-neither-safe-nor-secure/8005338>. [Accessed 14 January 2019].

[9] Office of the Australian Information Commissioner APP11 (2015). Security of Personal Information. [online] Available at: <oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>. [Accessed on 14 January 2019].

[10] Hicks, S. (2012). Russian Hackers Hold Gold Coast Doctors to Ransom. [online] Available at: <abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676>. [Accessed 14 January 2019].

[11] Department of Health (2013). Get your personal eHealth record now, Canberra: Department of Health. [online] Available at <www.ehealth.gov.au>. [Accessed 10 March, 2017].

[12] Glance, D. (2013). Is the government's missed health record target meaningful?, The Conversation, Melbourne.

[13] Dunlevy, S. (2015). Taxpayers have spent more than $1 billion on a digital health record that doctors won't use, News.Com. Melbourne.

[14] Donovan, J. (2010). eHealth: the advantages for consumers, Health Voices. Canberra.

[15] Department of Health Aging (2013). Get your personal eHealth record now, Canberra: Department of Health Aging. [online] Available at: <www.ehealth.gov.au> [Accessed 28 June 2014].

[16] Ohno-Machadoa, L., Silveira, P. S. P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. International Journal of Medical Informatics, 73(7-8), 599-606.

[17] Bosch, M., Faber, M. J., Cruijsberg, J., Voerman, G. E., Leatherman, S., Grol, R. P., Hulscher, M., & Wensing, M. (2009). Review article: Effectiveness of patient care teams and the role of clinical expertise and coordination: A literature review. Med. Care Res. and Rev.

[18] Kannampallil, T. G., Schauer, G. F., Cohen, T., & Patel, V. L. (2011). Considering complexity in health care systems. J.Biomed. Informatics.

[19] Malin, B., Nyemba, S., & Paulett, J. (2011). Learning relational policies from electronic health record access logs, J. Biomed. Informatics.

[20] AHIMA (2013). Integrity of the Health care Record: Best Practices for EHR Documentation, Ahima library. [online] Available at: <http://library.ahima.org/doc? oid=300257#.XD52XZUUmUk>. [Accessed 16 January 2019].

[21] Charles S. (2018). EHR vs. EMR: Is there any difference?, Technology Advice. [online] Available at: <https://technologyadvice.com/blog/health care/ehr-vs-emr/>. [Accessed on 29 January 2019].

[22] Health care Specialist (2018). Electronic Medical Records vs. Electronic Health Records – what is the difference?, revanuexl. [online] Available at:

<https://www.revenuexl.com/resources/emr-software-vs-ehr-software>. [Accessed on 27 January 2019].

[23] Weber-Jahnke, J., & Williams, J. (2010). Regulation of Patient Management Software. Health Law Journal.

[24] HealthTimes (2016). Practice management software comparison, HealthTimes. [online] Available at: <https://healthtimes.com.au/hub/health care-it/29/guidance/nc1/practice-management-software-comparison/1691/>. [Accessed 12 January 2019].

[25] Australian Family Physician (2011). Australia's systems of primary health care The need for improved coordination and implications for Medicare Locals. [online] available at: <https://www.racgp.org.au/afp/2011/december /australia%E2%80%99s-systems-of-primary-health care/>. [Accessed 11 January 2019].

[26] Bosch, M., Faber, M. J., Cruijsberg, J., Voerman, G. E., Leatherman, S., Grol, R. P., Hulscher, M., & Wensing, M. (2009). Review article: Effectiveness of patient care teams and the role of clinical expertiseand coordination: A literature review. Med. Care Res. and Rev.

[27] Kannampallil, T. G., Schauer, G. F., Cohen, T., & Patel, V. L. (2011). Considering complexity in health care systems. J. Biomed. Informatics.

[28] Malin, B., Nyemba, S., & Paulett, J. (2011). Learning relational policies from electronic health record access logs. J. Biomed. Informatics.

[29] Reynolds, P. (2004). The keys to identify: as health care organisations strive for greater security, some are using a very personal approach in the form of biometrics. Health management technology, 25 (12, 12 (14).

[30] Coiera, E. (2003). A guide to health informatics (2nd ed.). London: Arnold.

[31] Almunawar, N., & Anshari, M. (2012). Health Information Systems (HIS): Concept and Technology, research gate.

[32] Yazdi-Feyzabadi, V., Emami, M., & Mehrolhassani, M. H. (2015). Health Information System in Primary Health Care: The Challenges and Barriers from Local Providers' Perspective of an Area in Iran, International Journal of Preventive Medicine. US National Library of Medicine National Institutes of Health.

[33] Haux, R. (2006). Health information system – past, present, future. International Journal of Medical Informatics, 75 (3-4), 268-281.

[34] Nygren, E., Johnson, M., & Henriksson, P. (1992). Reading the medical record. II. Design of a human-computer interface for basic reading of computerized medical records. Computer Methods Programs Biomed. 39:13-25.

[35] Tange, H. J. (1994). The paper-based patient record: is it really so bad?. In Proceedings of the Twelfth International Congress of the European Federation for Medical Informatics. Lisbon, pp 459–63.

[36] Australian Nursing and Midwifery Federation e-Health Part 1: current state of play (2013). Australian Nursing Journal. 20 (2): 20. [online] Available at: <www.ajan.com.au/Vol34/Issue4/34-4.pdf> [Accessed 12 May 2017].

[37] Spriggs, M., Arnold, M. V., Pearce, C., & Fry, C. (2012). Ethical Questions Must be Considered for Electronic Health Records. Journal of Medical Ethics. 38 (9): 535–539.

[38] NEHTA (2013). What is a PCEHR?, National E-Health Transition Authority (NEHTA). [online] Available at: <https://www.aph.gov.au/Parliamentary_ Business /Senate_Estimates/clacctte /estimates/bud1314/NEHTA/index>. [Accessed 12 May 2013].

[39] Australian Digital Health Agency (2017). PCEHR Architecture, Australian government Canberra, [online] Available at: https://www.digitalhealth.gov.au/implementation-resources/ehealth-foundations/pcehr-architecture [Accessed 06 January 2018].

[40] Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Sakamoto, N., & Yamamoya, R. (2000). Architecture for networking electronic patient records systems. International journal of medical informatics, 69 (2), 161-167.

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

[42] Anderson, J. G. (2007). Social, Ethical and Legal Barriers to E-health. International Journal of Medical Informatics, 76 (5-6), 480-483.

[43] Conrick, M., & Newell, C. (2006). Health Informatics: Transforming Health care with Technology. Issues of Ethics and La. In M. Conrick (Ed.) Melbourne: Thomson Social Science Press.

[44] Blobel, B., Nordberg, R., Davis, J. M., & Pharow, P. (2006). Modelling privilege management and access control. International Journal of Medical Informatics, 75 (8), 597-623.

[45] Lopez, D. M., & Blobel, B. G. M. E. (2009). A development framework for semantically interoperable health information systems. International Journal of Medical Informatics, 78(2), 83-103.

[46] Christiansen, J. R. (1999). Why health care information isn't property: and why that is to everyone's benefit. Health Law Digest. American Health Lawyers Association, Washington, DC.

[47] Rodwin, M. A. (2009). The case for public ownership of patient data. JAMA. 302(1):86–88.

[48] Sitting, D. F., & Singh, H. (2011). Legal, Ethical and Financial Dilemmas in Electronic Health Record and Adoption and Use. US National Institutes of Health, Peadiatrics 127 (4).

[49] Sweeney, L. (2002). K-anonymity: a model for protecting privacy. IJUFKS. 10(5): 557–570.

[50] Gostin, L. O., & Nass, S. (2009). Reforming the HIPAA privacy rule: safeguarding privacy and promoting research. JAMA. 301(13):1373– 1375.

[51] Rosenbaum, S., Abramson, S., & MacTaggart, P. (2009). Health information law in the context of minors. Pediatrics. 123 (suppl 2):S116–S121.

[52] Berlan, E. D., & Bravender, T. (2009). Confidentiality, consent, and caring for the adolescent patient. Curr Opin Pediatr.21(4):450–456.

[53] US Council (2009). Council on Clinical Information Technology Policy statement: using personal health records to improve the quality of health care for children. Pediatrics. 124(1):403–409.

[54] Smith, P.C., Araya-Guerra, R., Bublitz, C., Parnes, B., Dickinson, L. M., Van Vorst, R., Westfall, J. M., & Pace, W. D. (2005). Missing clinical information during primary care visits. JAMA. 293(5):565–571.

[55] Foundation of Research and Education of AHIMA (2005). Update: maintaining a legally sound health record: paper and electronic. J AHIMA.76 (10): 64A– 64L.

[56] Singh, H., Thomas, E. J., Sittig, D. F., Wilson, L., Espadas, D., Khan, M. M., & Petersen, L. A. (2010). Notification of abnormal lab test results in an electronic medical record: do any safety concerns remain? Am J Med. 123(3):238–244.

[57] Federal Rules of Civil Procedure (2017). Producing documents, electronically stored information, and tangible things, or entering onto land, for inspection and

other purposes. Available at: <www.law.cornell.edu/rules/frcp/Rule34.htm> . [Accessed January 9, 2018].

[58] Miller, A. R., & Tucker, C. E. (2009). Electronic discovery and electronic medical records: does the threat of litigation affect firm decisions to adopt technology? Washington, DC: Federal Trade Commission.

[59] Hoffman, S., & Podgurski, A. (2009). E-Health hazards: provider liability and electronic health record systems. Berkeley Technology Law Journal. 24(4):1523–1581

[60] Mangalmurti, S. S., Murtagh, L., & Mello, M. M. (2010). Medical malpractice liability in the age of electronic health records. N Engl J Med. 363(21):2060–2067.

[61] McLean, T. R., Burton, L., Haller, C. C., & McLean, P. B. (2008). Electronic medical record metadata: uses and liability. Am Coll Surg. 206 (3):405–411.

[62] Koppel, R., Metlay, J. P., Cohen, A., Abaluck, B., Localio., A. R., Kimmel, S. E., & Strom, B. L. (2005). Role of computerized physician order entry systems in facilitating medication errors. JAMA. 293(10):1197–1203.

[63] Nebeker, J. R., Hoffman, J. M., Weir, C. R., Bennett, C. L., & Hurdle, J. F. (2005). High rates of adverse drug events in a highly computerized hospital. Arch Intern Med.165(10): 1111–1116.

[64] Johnson, C. W. (2009). Politics and patient safety don't mix: understanding the failure of large-scale software procurement for health care systems. Fourth IET Systems Safety Conference. Savoy Place, London.

[65] Koppel, R., & Kreda, D. (2009). Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. JAMA. 301(12): 1276–1278.

[66] Hoffman, S., & Podgurski, A. (2008). Finding a cure: the case for regulation and oversight of electronic health record systems. Harvard Journal of Law and Technology. 22(1): 103–165.

[67] Sittig, D. F., & Classen, D. C. (2010). Safe electronic health record use requires a comprehensive monitoring and evaluation framework. JAMA.303(5):450–451.

[68] Ohno-Machadoa, L., Silveira, P. S. P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. International Journal of Medical Informatics, 73 (7-8), 599-606.

[69] Garson, K., & Adams, C. (2008). Security and privacy system architecture for an e-hospital environment. Paper presented at the Proceedings of the 7th symposium on identity and trust on the Internet, Gaithersburg, Maryland.

[70] Blobel, B., & Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems. International Journal of Medical Informatics 62 (1), 51-78.

[71] Shin, Y. N., Lee, Y. J., Shin, W., & Choi, J. (2008). Designing Fingerprint – Recognition- Based Access Control for Electronic Medical Records Systems. 2nd International Conference on Advanced Information Networking and Applications Workshops, Okinawa, Japan.

[72] Weir, C. R. (2003). Direct text entry in electronic progress notes. An evaluation of input errors. Methods Inf Med.

[73] Shu, J. (2018). Privacy-Preserving Task Recommendation Services for Crowd sourcing. IEEE Transactions on Services Computing. doi:0.1109/ TSC.2018.2791601.

[74] Wang, H., Cao, J., & Zhang, Y. (2002). Ticket-based service access scheme for mobile users. Australian Computer Science Communications 24 (1), pp: 285-292.

[75] Australian Government (2013). The eHealth consultation [online], available at: <http://www.health.gov.au/ internet/main/ publishing.nsf /Content/ pacd- ehealth-consultation-faqs>. [Accessed 15 March 2015]

[76] American Health Information Management Association (2012). AHIMA Data Quality Management Model. Available at: <http://library.ahima.org/PB/DataQualityModel>. [Accessed 12 December 2018].

[77] Mark, E., & Serge, B. (2004). A case study in access control requirements for a Health Information System. In Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation – Vol. 32, pp: 53-61.

[78] Vimalachandran, P., Wang, H., Zhang, Y., & Zhuo, G. (2016). The Australian PCEHR System: Ensuring Privacy and Security through an Improved Access Control Mechanism. EAI Endorsed Trans. Scalable Information Systems 3 (8), e4.

[79] Vimalachandran, P., Wang, H., Zhang, Y., Zhuo, G., & Kuang, H. (2017). Cryptographic Access Control in Electronic Health Record Systems: A Security Implication. Web Information Systems Engineering – WISE 2017: 18th

International Conference, Puschino, Russia. Proceedings, Part II. WISE (2) : 540-549

[80] Donovan, J. (2010). eHealth: the advantages for consumers, Health Voices. Canberra.

[81] Department of Health (2015). My Health Record. [online] Available at: <https://myhealthrecord.gov.au/internet /ehealth/publishing.nsf/Content/faqs-individuals-gen>. [Accessed 2 May 2016].

[82] CSC Health care (2010). A Rising Tide of Expectations: Australian consumers' views on electronic health records – a necessary ingredient in health care reform, CSC Health care. Sydney.

[83] Glance, D. (2015). New name and opt- out policy won't save the personal health record. [online] Available at: <http://the conversation.com/new- name-and-opt-out-policy-wont- save-the-personal-health-record-41601>. The conversation, Melbourne. [Accessed 2 May 2016).

[84] AMA (2012). Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System, AMA. Canberra. pp 17 -19.

[85] Dolin, R. H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F. M., Biron, P. V., & Shabo A. (2006). HL7 Clinical Document Architecture, Release 2. Journal of the American Informatics Association, 13 (1).

[86] Guo, J., Takada, A., Niu, T., He, M., Tanaka, K., Sato, J., Suzuki, T., Nakashima, Y., Araki, K., & Yoshihara, H. (2005). Enhancement of MML Medical Data Exchange Standard for localized Chinese version. Journal of Medical System, 29 (5), 555-567.

[87] Guo, J., Takada, A., Tanaka, K., Sato, J., Suzuki, M., Suzuki, T., Nakashima, Y., Araki, K., & Yoshihara, H. (2004). The development of a MML (Medical Markup Language) Version 3.0 as a medical document exchange format for HL7 message. Journal of Medical Systems, 28(6), 523-533.

[88] New London Consulting (2012). Australia: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes. Fair Warning. Australian Patient Survey.

[89] Department of Defence (2012). Cloud Computing Security Considerations. Cyber Security Operations Centre, Australian Government, Canberra.

[90] Computer Security Resource Center (2018). Cloud Computing. National Institute of Standards and Technology, U. S. Department of Commerce.

[91] Kenn, P. G. W. (1987). MIS research: Current status, trends and needs. Information systems education: Recommendations and implementation (pp 1-13), Cambridge, England: Cambridge University.

[92] Burstein, F., & Gregor, S. (1999). The Systems Development or Engineering Approach to Research in Information Systems: An Action Research Perspective. Paper presented at the Proc. 10th Australian Conference on Information Systems. Available at: <https://www.researchgate.net/publication/228604095_The_systems_development_or_engineering_approach_to_research_in_information_systems_An_action_research_perspective>. [Accessed 21 January 2019].

[93] Parker, C., Wafula, E., & Swatman, P (1994). Information systems research methods: The technology transfer problem. Paper presented at the 5th Australian Conference on Information System, Caulfield, Vic., Monash University, Department of Information Systems.

[94] Nunamaker, J. F., Chen, M., & Purdin, T. (1991). Systems development in information systems research. Journal of Management Information systems, 7(3), 89-106.

[95] Harris, S. (2005). All-in-one CISSP Exam Guide, Third Edition, McGraw Hill Osborne, Emeryvill, California.

[96] The Thames Valley Police (n.d.). Business Crime: Access Control. [online] Available at: http://www.thamesvalley.police.uk/reduction/businesscrime/access.htm, U.K [Accessed on 12 July 2014].

[97] The Sapior Company (2007). Enabling Ethical Data Sharing and Pseudonymisation. [online] Available at: www.sapior.com, U.K. [Accessed 12 June 2014].

[98] RU Evaluation Secure Ltd (n.d.). Data Encryption. [online] Available at: http://www.yourwindow.to/information-security/gl_dataencryption.htm [Accessed 18 June 2014].

[99] David Litchfield (2006). Understanding Database Security and which database is more secure? Oracle vs. Microsoft. [online] Available at: www.davidlitchfield.com. [Accessed 22 December 2018].

[100] Wiedman, B. (2009). Database Security – Common-sense Principles.

[101] Castano, S., Fugini, M. G., Martella, G., & Samarati, P. (1995). Database Security. Addison-Wesley & ACM Press.

[102] Chapple, M. (2007). SQL Injection Attacks on Databases, available at <http://databases.about.com/od/security/a/sqlinjection.htm>, NY. [Accessed 12 December 2018].

[103] PHP manual (2007). About Database Security. [online] Available at: <http://www.science.uva.nl/ict/ossdocs/php4/security.database.html> [Accessed on 15 June 2018].

[104] Trinanes, J. A. (n.d.), Database Security in High Risk Environment. [online] Available at: <http://www.governmentsecurity.org/articles/Database Security in High RiskEnvironments.php>

[105] Horn, T. V. (2007). Database Security. [online] Available at: <http://www.databasejournal.com/news/article.php/3657096>, U.S.A. [Accessed 10 September 2018].

[106] Beaver, K. (June 2007). Database Threats Include Unruly Insiders. [online] Available at: <http://searchsqlserver.techtarget.com/tip /0,289483,sid87_gci1261129,00.html>, U.S.A. [Accessed 10 September 2018.

[107] Space, D. (2007). RDBMS and Storage Layer. [online] Available at: <http://www.dspace.org/index.php?option=com_content&task = view&id=154>. [Accessed on 22 June 2018].

[108] Kenan, K. (2006). Cryptography in the Database: The Last Line of Defense, Symantec Press.

[109] Denning, D. E. R. (1982), Cryptography and Data Security, Addison-Wesley.

[110] Gollmann, D. (August 1999), Computer Security. John Wiley and Sons. NJ.

[111] Kabay, M. E.(1996), The NCSA Guide to Enterprise Security: Protecting Information Assets. McGraw-Hill. NY.

[112] IT Security web site, (2007), Security Threats. [online] Available at: <http://www.itsecurity.com/features/network-security-threats-011707/> NY. [Accessed on 18 July 2018].

[113] Sahar, M. (March 2007). Threats to Information Security. [online] Available at: <http://www.shvoong.com/exact-sciences/490867-threats-information-security/>. [Accessed on 12 July 2018]

[114] Gollmann, D. (2006), Computer Security, 2nd Ed., Wiley. NJ.

[115] Delfs, H. & Knebl, H. (2002). Introduction to Cryptography: Principles and Applications, Springer.

[116] Mamykina, L., Vawdrey, D. K., Stetson, P. D., Zheng, K., & Hripcsak, G. (2012). Clinical documentation: composition or synthesis?, J Am Med Inform Assoc.

[117] Love, J. S., Wright, A., Simon, S. R., Jenter, C. A., Soran, C. S., Volk, L. A., Bates, D. W., & Poon, E. G. (2012). Are physicians' perceptions of health care quality and practice satisfaction affected by errors associated with electronic health record use? Am Med Inform Assoc.

[118] Sittig, D. F., & Singh, H. (2011) Defining health information technology-related errors: new developments since to err is human. Arch Intern Med.

[119] Hoffman, S., & Podgurski, A. (2008), Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems. Harvard Journal of Law and Technology.

[120] Phillips, W., & Fleming, D. (2009). Ethical concerns in the use of electronic medical records. Pub Med. National Institute of Health. Bethesda MD.

[121] Weir, C. R, Hurdle, J. F., Felgar, M. A., Hoffman, J. M., Roth, B., & Nebeker, J. R. (2003). Direct text entry in electronic progress notes. An evaluation of input errors. Methods Inf Med.

[122] Coiera, E., Westbrook, J. I., & Wyatt, J. C. (2006). Safety and Quality of Decision Support Systems. Yearbook of Medical Informatics.

[123] Australian Government (2013). The eHealth consultation. [online] Available at: <http://www.health.gov .au/ internet/main/ publishing.nsf/Content/pacd-ehealth-consultation-faqs> [Accessed 15 March 2015].

[124] Office of theAustralians Information Commissioner (2012). [online] Available at: <http://www.oaic.gov.au/privacy/privacy-topics/health-for-individuals/health care-identifiers> [Accessed 20 August 2015].

[125] Australian Government (2013), Health care Identifiers Services. [Online] Available at: <http://www. humanservices.gov.au/customer/services/medicare /health care-identifiers-service#a2> [Accessed 24 November 2016].

[126] NEHTA (2015). Health care Identifiers Implementation Guide - NEHTA, [online] Available at: <www.nehta.gov.au/.../1319--health care-identifiers-implementation-guide> [Accessed 12 September 2015].

[127] Phillips, W., & Fleming, D. (2009). Ethical concerns in the use of electronic medical records. Mo Med.

[128] American Health Information Management Association (2012). AHIMA Data Quality Management Model.

[129] Hicks, S. (2012). Russian hackers hold Gold Coast doctors to ransom ABC, [online] Available at: <http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676> [Accessed 11 August 2015].

[130] Hammond, K. W., Helbig, S. T., Benson, C. C., & Brathwaite-Sketoe, B. M. (2003). Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting, and Duplication.

[131] Vimalachandran, P., Wang, H., & Zhang, Y. (2015). Securing Electronic Medical Record and Electronic Health Record Systems through an Improved Access Control. The 4th International Health Information Science Conference (HIS), Melbourne, 9085, 17-30.

[132] Kannry, J. (2011). Effect of E-Prescribing Systems on Patient Safety. Mount Sinai Journal of Medicine. National Institutes of Health. NJ.

[133] Sun, X., Wang, H., Li, J., & Zhang, Y. (2012). Satisfying privacy requirements before data anonymization, The Computer Journal 55 (4), 422-437.

[234] Kabir, M. E., Wang, H., & Bertino, E. (2011). Efficient systematic clustering method for k-anonymization, ActaInformatica 48 (1), 51-66.

[135] Wang, H., Cao, J., & Zhang, Y. (2001). A consumer scalable anonymity payment scheme with role based access control, Web Information Systems Engineering.

[136] Wang, H., Cao, J., & Zhang, Y. (2005). A flexible payment scheme and its role-based access control, IEEE Transactions on knowledge and Data Engineering 17 (3), 425-436.

[137] Acheson, E. & Evans, J. (1964). The oxford record linkage study: A review of the method with some preliminary results. Proceedings of the Royal Society of Medicine, page 269–274.

[138] Ben-Assuli, O., Shabtai, I., & Leshno. M. (2015). Using electronic health record systems to optimize admission decisions: The Creatinine case study. Health Informatics J, 21(1):73-88.

[139] Byrne, C. M., Mercincavage, L. M., Bouhaddou, O., Bennett, J. R., Pan, E. C., Botts, N. E., Olinger, L. M., Hunolt, E., Banty, K. H., & 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. Int J Med Inform. August; 83(8):537-47.

[140] Giokas, D. (2005). Canada Health Infoway - Towards a National Interoperable Electronic Health Record (EHR) Solution. Stud Health Technol Inform, 115:108-40.

[141] Pearce, C., & Bainbridge, M. (2014). A personally controlled electronic health record for Australia. J Am Med Inform Assoc, 21(4):707-13.

[142] Tiik, M., & Ross, P. (2010). Patient opportunities in the Estonian Electronic Health Record System. Stud Health Technol Inform, 156:171-7.

[143] Tierney, W. M., Rotich, J. K., Smith, F. E., Bii, J., Einterz, R. M., & Hannan, T. J. (2002). Crossing the "digital divide:" implementing an electronic medical record system in a rural Kenyan health center to support clinical care and research. Proc AMIA Symp, 792-5.

[144] Sek, A. C., Cheung, N. T., Choy, K. M., Wong, W. N., Tong, A. Y., Fung, V. H., Fung, M., & Ho, E. (2007). A territory-wide electronic health record--from concept to practicality: the Hong Kong experience. Stud Health Technol Inform, 129 (Pt 1): 293-6.

[145] Li, Y. C., Lee. P. S., Jian, W. S., & Kuo, C. H. (2009). Electronic health record goes personal world-wide. Yearb Med Inform, 40-3.

[146] Iakovidis, I. (1998). From electronic medical record to personal health records: present situation and trends in European Union in the area of electronic health care records. Stud Health Technol Inform, 52 Pt 1: suppl 18-22.

[147] Baudendistel, I., Winkler, E., Kamradt, M., Brophy, S., Langst, G., Eckrich, F., Heinze, O., Bergh, B., Szecsenyi, J., & Ose, D. (2015). The patients' active role in managing a personal electronic health record: a qualitative analysis. Support Care Cancer, (9):2613-21.

[148] Buckley, A., & Fox, S. (2015). Know me - a journey in creating a personal electronic health record. Stud Health Technol Inform 2015; 208: 93-7.

[149] Cahill, J. E., Gilbert, M. R., & Armstrong, T. S. (2014). Personal health records as portal to the electronic medical record. J Neurooncol, 117(1): 1-6.

[150] Wallace, S., Clark, M., & White, J. (2012). It's on my iPhone: attitudes to the use of mobile computing devices in medical education, a mixed-methods study. BMJ Open, 2, e001099.

[151] Aungst, T. D. (2013). Medical applications for pharmacists using mobile devices. Ann Pharmacother, 47(7–8):1088–1095.

[152] Kiser, K. (2011). 25 ways to use your smartphone. Physicians share their favorite uses and apps. Minn Med, 94(4): 22–29.

[153] Ozdalga, E., Ozdalga, A., & Ahuja, N. (2012). The smartphone in medicine: a review of current and potential use among physicians and students. J Med Internet Res, 14(5):e128.

[154] Yoo, J. H. (2013). The meaning of information technology (IT) mobile devices to me, the infectious disease physician. Infect Chemother, 45(2): 244– 251.

[155] O'Neill, K. M., Holmer, H., Greenberg, S. L., & Meara, J. G. (2013). Applying surgical apps: Smartphone and tablet apps prove useful in clinical practice. Bull Am Coll Surg, 98 (11):10–18.

[156] Mosa, A. S., Yoo, I., Sheets, L. (2012). A systematic review of health care apps for smartphones. BMC Med Inform Dec Mak, 12:67.

[157] Divali, P., Camosso-Stefinovic, J., & Baker, R. (2013). Use of personal digital assistants in clinical decision making by health care professionals: a systematic review. Health Informatics J, 19 (1): 16–28.

[158] Murfin, M. (2013). Know your apps: an evidence-based approach to the evaluation of mobile clinical applications. J Physician Assist Educ, 24(3):38–40.

[159] Mickan, S., Tilson, J. K., Atherton, H., Roberts, N. W., & Heneghan, C. (2013). Evidence of effectiveness of health care professionals using handheld computers; a scoping review of systematic reviews. J Med Internet Res, 15 (10): e212.

[160] Misra, S., Lewis, T. L., & Aungst, T. D. (2013). Medical application use and the need for further research and assessment for clinical practice: creation and integration of standards for best practice to alleviate poor application design. JAMA Dermatol, 149 (6): 661–662.

[161] Boulos, M. N., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory health care; an overview, with example from eCAALYX. Biomed Eng Online.

[162] Chase, J. (2013). IPads and other drugs- Medical Marketing & Media: The Interactive Guide.10–11.

[163] Moodley, A., Mangino, J., & Goff, D. (2013). Review of infectious diseases applications for iPhone/iPad and Android: from pocket to patient. Clin Infect Dis. 57: 1145–1154.

[164] Australian Government (2018). Notifiable Data Breaches scheme, Office of the Australian Information Commissioner. [Online] Available at: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme> [Accessed 07 February 2019].

[165] Australian Digital Health Agency (2018). Australian Parliament passes legislation to strengthen My Health Record privacy, Australian Government. [online] Available at: <https://www.myhealthrecord.gov.au/news-and-media/my-health-record-stories/legislation-strengthens-privacy> [Accessed 12 December 2018].

[166] Federal Register of Legislation (2017). My Health Record Act 2012, Australian Government. [online] Available at: <https://www.legislation.gov.au/Details/C2017C00313> [Accessed 07 February 2019].

[167] Brose, G. (2011). Access control. In Encyclopedia of Cryptography and Security, Springer US pages 2–7. [online] Available at: <http://dx.doi.org/ 10.1007/ 978-1-4419- 5906-5_179> [Accessed 12 January 2018].

[168] Deng, M., DeCock, D. & Bart, P. (2009). Towards a cross-context identity management framework in e-health. Online Information Review, 33, pages 422–442.

[169] Narayan, S., Gagne, M., & Safavi-Naini, R. (2010). Privacy preserving EHR system using attribute-based infrastructure. Proceedings of 19th ACM workshop on Cloud computing security workshop, CCSW '10, New York, NY, USA, ACM, pages 47–52.

[170] Lohr, H., Sadeghi, A. R., & Winandy, M. (2010). Securing the e-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium, IHI New York, NY, USA, ACM, 220–229.

[171] Yu, W., & Chekhanovskiy, M. (2007). An electronic health record content protection system using smartcard and pmr. e-Health Networking, Application and Services. The 9th International Conference on, pages 11 –18.

[172] Microsoft HealthVault (2013). Health Vault. [online] Available at: <http://healthvault.com>. [Accessed 22 January 2019].

[173] Dossia (2013). Employer q and a - dossia personal health platform. [Online]. Available at: <http://www.dossia.es/for-employers/employer-q-and-a>. [Accessed 12 November 2018]

[174] GNU Health (2013). GNU Health. [Online] Available at: <http://health.gnu.org/>. [Accessed 16 November 2018]

[175] Google Inc. (2013). Google Health - About. [Online] Available at: <http://www.google.com/intl/en_us/health/about/> [Accessed 12 November 2018].

[176] Brown, A., & Weihl, B. (2011). Official Google Blog: An update on Google Health and Google Power Meter. [Online] Available at: <http://googleblog.blogspot.fi/2011/06/update-on-google-health-and-google.html> [Accessed 12 January 2018].

[177] Microsoft (2013). HealthVault FAQs. [Online] Available at: <http://msdn.microsoft.com/en-us/healthvault/cc196394.aspx>. [Accessed 12 November 2018].

[178] Masi, M., Pugliese, R., & Tiezzi, F. (2009). On secure implementation of an ihe xua-based protocol for authenticating health care professionals. Proceedings of the 5th International Conference on Information Systems Security, ICISS, Berlin, Heidelberg, Springer-Verlag, pages 55–70. [Online] Available at: <http://dx.doi.org/10. 1007/978-3-642-10772-6_6>. [Accessed 12 December 2018].

[179] Williams, J. (2010). Social networking applications in health care: threats to the privacy and security of health information. Proceedings of the ICSE Workshop on Software Engineering in Health Care, SEHC, New York, NY, USA, ACM, 39–49. [online]. Available at: <http://doi.acm.org/10.1145/1809085.1809091>. [Accessed 12 December 2018].

[180] Waegemann, P. (2003). EHR vs. CPR vs. EMR. Health care Informatics [Online]. Available at: <http://www.health careinformatics.com/issues/2003/05_03/cover_ehr.htm>. [Accessed 6 December 2018].

[181] Bakker, A. (2004). Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. International Journal of Medical Informatics. 2004; 73:267-270.

[182] Anderson, R. (2001). Security Engineering: A guide to build dependable distributed systems. Wiley. NJ.

[183] Blobel, B. (2004). Authorisation and access control for electronic health record systems. International Journal of Medical Informatics, 73: 251-257.

[184] Rissanen, E., Firozabadi, S., & Sergot, M. (2004). Towards a Mechanism for Discretionary Overriding of Access Control. Proceedings of the 12th International Workshop on Security Protocols, Cambridge.

[185] Buntin, M. B., Jain, S. H., & Blumenthal, D. (2010). Health information technology: Laying the infrastructure for national health reform. Health Affairs 29, 6, 1214–1219.

[186] Ludwick, D. A. & Doucette, J. (2009). Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int. J. Med. Informatics78, 1, 22–31.

[187] Pizziferri, L., Kittler, A. F., Volk, L. A., Honour, M. M., Gupta, S., Wang, S., Wang, T., Lippincott, M., Li, Q., & Bates, D. W. (2005). Primary care physician

time utilization before and after implementation of an electronic health record: A time-motion study. J. Biomed. Informatics 38, 3, 176–188.

[188] Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S. C., & Shekelle, P. G. (2006). Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. Ann. Intern. Med. 144, 10, 742–752.

[189] Bosch, M., Faber, M. J., Cruijsberg, J., Voerman, G. E., Leatherman, S., Grol, R. P., Hulscher, M., & Wensing, M. (2009). Review article: Effectiveness of patient care teams and the role of clinical expertise and coordination: A literature review. Med. Care Res. and Rev. 66, 6 Suppl., 5S–35S.

[190] Kannampallil, T. G., Schauer, G. F., Cohen, T., & Patel, V. L. (2011). Considering complexity in health care systems. J. Biomed. Informatics 44, 6, 943–947.

[191] Malin, B., Nyemba, S., & Paulett, J. (2011). Learning relational policies from electronic health record access logs. J. Biomed. Informatics 44, 2, 333–342.

[192] Ash, J. S., Berg, M., & Coiera, E. (2004). Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. J. Amer. Med. Informatics Assoc. 11, 2, 104–112.

[193] Goldschmidt, P. G. (2005). Hit and mis: Implications of health information technology and medical information systems. Comm. ACM 48, 10, 68–74.

[194] Campbell, H., Hotchkiss, R., Bradshaw, N., & Porteous, M. (1998). Integrated care pathways increase use of guidelines. British Med. J. 316, 133–137.

[195] King, J. T., Smith, B., & Williams, L. (2012). Modifying without a trace: General audit guidelines are inadequate for open-source electronic health record audit mechanisms. In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium. 305–314.

[196] Appari, A., & Johnson, M. (2011). Information security and privacy in health care: Current state of research. Int. J. Internet Enterprise Manage. 6, 279–314.

[197] Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Syst. 49, 138–150.

[198] Davis, D., & Having, K. (2006). Compliance with HIPAA security standards in U.S. hospitals. J. Health care Inform. Manage. 20, 108–115.

[199] Kwon, J., & Johnson, M. (2013). Security practices and regulatory compliance in the health care industry. J. Amer. Med. Informatics Assoc. 20, 1, 44–50.

[200] Smith, E., & Eloff, J. (1999). Security in health-care information systems - Current trends. Int. J. Med. Informatics 54, 39–54.

[201] Manos, D. (2012). Four reasons for CIOs to celebrate stage two meaningful use. Gov. Health IT Mag.

[202] Probst, C. W., Hansen, R. R., & Nielson, F. (2007). Where can an insider attack? In Proceedings of the 4th International Conference on Formal Aspects in Security and Trust. 127–142.

[203] Schultz, E. (2002). A framework for understanding and predicting insider attacks. Comput. Security 21, 526–531.

[204] Stolfo, S., Bellovin, S., Hershkop, S., Keromytis, A., Sinclair, S., & Smith, S. (2008). Insider Attack and Cyber Security: Beyond the Hacker. Springer, New York, NY.

[205] Amatayakul, M. (2009). Think a privacy breach couldn't happen at your facility? Hospital Financial Manage.12, 61–65.

[206] Dimick, C. (2010). A guide to California's breaches: First year of state reporting requirement reveals common privacy violations. J. Amer. Health Inform. Manage. Assoc. 81, 34–36.

[207] Loomis, G. A., Ries, J. S., Saywell, R. M., & Thakker, N. R. (2002). If electronic medical records are so great, why are not family physicians using them? J. Family Practice 51, 7, 636–641.

[208] Goldberg, I. V. (2000). Electronic medical records and patient privacy. Health Care Manager 18, 3, 63–69.

[209] HTO (2009). Health care SaaS Vs. Licensed Software, Health care Technology Online.

[210] HITECH (2010). Meeting HITECH's Challenge to the Health Care Industry, An Oracle White Paper.

[211] Reinhardt, A. B. (2001). CoSAWoE – A Model for Context-sensitive AccessControl in Workflow Environments, South Africa.

[212] Elsenpeter, R., Velte, T. A., & Velte, T. J. (2010). Cloud Computing a Practical Approach, McGraw Hill.

[213] Pfleger, C. P. (1997). Security in Computing, 2nd Edition, Prentice-Hall International Inc., Englewood Cliffs, NJ.

[214] Jiang, H., & Lu, S. (2006). RTFW: An Access Control Model for Workflow Environment, Computer Supported Cooperative Work in Design, 10th International Conference on Computer Supported Cooperative Work in Design.

[215] Coyne, E., Fenstein, H., Sandhu, R., & Youman, C. (1996). Role-Based Access Control Models, IEEE Computer, 29(2):38-47.

[216] Edsberg, O., & Rostad, L. (2006). A Study of Access Control Requirements for Health care Systems Based on Audit Trails from Access Logs, In Proc. of 22nd Annual Computer Security Applications Conference, Miami, Florida.

[217] OpenEHR Community (2010). openEHR. [online] Available at: <http://www.openehr.org>. [Accessed 22 January 2019].

[218] Dolin, R. H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F. M., & Biron, P. V. (2004). HL7 clinical document architecture, release 2.0. ANSI Standard.

[219] Eyers, D. M., Bacon, J., & Moody, K. (2006). OASIS role-based access control for electronic health records. In IEEE proceedings e software, p. 16e23.

[220] Becker, M. Y., & Sewell, P. (2004). Flexible trust management, applied to electronic health records. In: Proc. of IEEE 17th computer security foundations workshop, p. 139 -54.

[221] Bhatti, R., Moidu, K., & Ghafoor, A. (2006). Policy-based security management for federated health care databases (or RHIOs). In: Proc. of the international workshop on health care information and knowledge management. p. 41e8.

[222] Byun, J. W., Bertino, E., & Li, N. (2005). Purpose based access control of complex data for privacy protection. In: Proc. of 10th ACM symposium on access control models and technologies (SACMAT). p. 102e10.

[223] Yang, N., Barringer, H., & Zhang, N. (2007). A purpose-based access control model. In: Proc. of 3rd international symposium on information assurance and security (IAS). p. 143e8.

[224] American National Standards Institute (2004). American National Standard for Information Technology – Role Based Access Control. ANSI INCITS 359.

[225] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2): 38-47.

[226] Becker, M. Y., & Sewell, P. (2004). Flexible trust management, applied to electronic health records. In Proceedings of the 17th IEEE Computer Security Foundations Workshop, 139-154.

[227] Eyers, D. M., Bacon, J. & Moody, K. (2006). OASIS role-based access control for electronic health records. IEE Proceedings - Software, 153(1):16-23.

[228] Reid, J., Cheong, I., Henricksen, M., & Smith, J. (2003). A novel use of RBAC to protect privacy in distributed health care information systems. In Proceedings of the 8th Australasian Conference on Information Security and Privacy, 403-415.

[229] Rostad, L., & Edsberg, O. (2006). A study of access control requirements for health care systems based on audit trails from access logs. In Proceedings of the 22nd Annual Computer Security Applications Conference, 175-186.

[230] Cederquist, J. G., Corin, R., Dekker, M. A. C., Etalle, S., den Hartog, J. I., & Lenzini, G. (2007). Audit-based compliance control. International Journal of Information Security, 6(2-3):133-151.

[231] Dekker, M. A. C., & Etalle, S. (2007). Audit-based access control for electronic health records. Electronic Notes in Theoretical Computer Science, 168:221-236.

[232] Tolone, W., Ahn, G. J., Pai, T., & Hong, S. P. (2005). Access control in collaborative systems. ACM Comput. Surv., 37(1):29–41.

[233] Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003), Role-Based Access Control. Computer Security Series. Artech House Publishers, Boston, 1 edition. ISBN: 1580533701.

[234] Zhang, L., Ahn, G. J., & Chu, B. T. (2002). A role-based delegation framework for health care information systems. Proceedings of the seventh ACM symposium on Access control models and technologies. ACM Press, Monterey, California, USA.

[235] Na, S., & Cheon, S. (2002). Role delegation in role-based access control. Proceedings of the fifth ACM workshop on Role-based access control. ACM Press, Berlin, Germany.

[236] Barka, E., & Sandhu, R. (2000). Framework for role-based delegation models. In Annual Computer Security Applications Conference (ACSAC), pages 168–176.

[237] Dixon, P. (2006). Medical identity theft: The information crime that can kill you. The World Privacy Forum. [Online] Available at: <http://www.worldprivacyforum.org/medicali den-titytheft.html>, [Accessed 12 December 2018].

[238] Gayer, J. (2003). Policing privacy: Law enforcement's response to identity theft. CALPIRG Education Fund. [Online] Available at: <http://www.calpirg.org/home/reports/report archives> [Accessed 7 June 2018].

[239] McGuigan, C., & Browne, M. (2007). Hospital leak linked to witness in lvf case. Belfast Telegraph. [Online] Available at: <http://www.belfasttelegraph.co.uk /sundaylife/news/hospital-leak-linked-to-witness -in-lvf-case-13904797.html> [Accessed 7 June 2018].

[240] Baird, M. (2008). Personal files were accessible for more than three weeks. The Western Star. [Online] Available at: <http://www.thewesternstar.com/ index.cfm?sid-=104156&sc=23> [Accessed 5 February 2018].

[241] Johnson, E. (2009). Data haemorrhages in the health-care sector. In Financial Cryptography and Data Security. pp 71-89 ,5628.

[242] Long, J. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Press.

[243] Preimesberger, C. (2006). Cyber-criminals use p2p tools for identity theft, security analyst warns. eWeek.com.

[244] Ernst, F. R., & Grizzle, A. J. (2001). Drug-related morbidity and mortality: Updating the cost-of-illness model. Technical report.

[245] Ernst, F. R. & Grizzle, A. J. (1995). Drug-related morbidity and mortality: Updating the cost-of-illness model. Technical report.

[246] Powell, J. & Buchan, I. (2005). Electronic Health Records Should Support Clinical Research. Journal of Medical Internet Research, 7:e4.

[247] Pommerening, K. & Reng, M. (2004). Secondary use of the Electronic Health Record via pseudonymisation. Medical Care Compunetics 1, 441–446.

[248] Pommerening, K. (1994). Medical Requirements for Data Protection. In IFIP Congress, Vol. 2, pp 533–540.

[249] Taipale, K. (2004). Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd. International Journal of Communications Law & Policy, 9.

[250] Thielscher, C., Gottfried, M., Umbreit, S., Boegner, F., Haack, J., & Schroeders, N. (2005). Patent: Data processing system for patent data.

[251] Biskup, J., & Flegel, U. (2000). Transaction-based pseudonyms in audit data for privacy respecting intrusion detection. In RAID: Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, pages 28–48, London, UK. Springer-Verlag.

[252] Flegel, U. (2002). Pseudonymizing unix log files. In InfraSec ’02: Proceedings of the International Conference on Infrastructure Security, pages 162–179, London, UK. Springer-Verlag.

[253] Jorns, O., Bessler, S., & Pailer, R. (2004). An efficient mechanism to ensure location privacy in telecom service applications. In Net-Con. Mallorca, Spain.

[254] Jorns, O., Jung, O., Gross, J., & Bessler, S. (2005). A privacy enhancement mechanism for location based service architectures using transaction pseudonyms.

In 2nd International Conference on Trust, Privacy, and Security in Digital Business, Copenhagen, Denmark.

[255] Task Force on Medical Informatics (1996). Safeguard Needed in Transfer of Patient Data. PEDIATRICS Vol. 98 No. 5, pp. 984-986.

[256] Chadwick, D., & Mundy, D. (2004). The secure electronic transfer of prescriptions. Health care Computing.

[257] Huston, T. (2001). Security Issues for Implementation of E-medical Records. Communication of the ACM, 44(9) pp. 89-94.

[258] Stein, L. D. (1997). The Electronic Medical Record: Promises and Threats. Web Journal, 2(3)

[259] Evered, M., & Bogeholz, S. (2004). A case study in access control requirements for a health information system. Australasian Information Security Workshop.

[260] Reid, J., Cheong, I., Henricksen, M., & Smith, J. (2003). A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems. In Safavi-Naini, Rei and Seberry, Jennifer, Eds. Proceedings 8th Australasian Conference on Information Security and Privacy (ACISP 2003) 2727, pages 403-415, Wollongong.

[261] Motta, G. H. M. B., & Furuie, S. S. (2003). A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record. IEEE Transactions on Information Technology in Biomedicine 7(3):202-207.

[262] Khayat, E. J., & Abdallah, A. E. (2003). A formal model for flat role-based access control. IEEE International Conference on Computer Systems and Applications, Tunisia.

[263] Choudhri, A., Kagal, L., Joshi, A., Finin, T., & Yesha, Y. (2003). Patient Service: Electronic Patient Record Reaction and Delivery in Pervasive Environment. Fifth International Workshop on Enterprise Networking and Computing in Health care Industry, Healthcom.

[264] Buck, C. F. (2007). Designing a consumer-centred personal health record. Technical report, California Health Foundation.

[265] Kim, G. R., & Lehmann, C. U. (2008). Paediatric aspects of inpatient health information technology systems. In Paediatrics, volume 122.

[266] Lohr, C. (2009). G.E. and Intel join forces on health technologies. New York Times.

[267] Tripathi, M., Delano, D., Lund, B., & Rudolph, L. (2009). Engaging patients for health information exchange. Health Affairs, 28(2):435- 43.

[268] U.S. Department of Health and Human Services (2008). The nationwide privacy and security framework for electronic exchange of individually identifiable health information. The National Coordinator for Health Information Technology.

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

[270] Jin, J., Ahn, G. J., Hu, H., Convington, M. J., & Zhang, X. (2009). Patient-centric authorization framework for sharing electronic health records. In ACM SACMAT, pp 125-134.

[271] Mandi, K. D., Simons, W. W., Crawford, W. C. R., & Abbett, J. M. (2007). Indivo: a personally controlled health record for health information exchange and communication. BMC Medical Informatics and Decision Making.

[272] Mohan, A., Bauer, D., Blough, D. M., Ahamad, M., Bamba, B., Krishnan, R., Liu, L., Mashima, D., & Palanisamy, B. (2009). A patient-centric, attribute-based, source-variable framework for health record sharing. In GIT CERCS Technical Report No. GIT-CERCS-09-11.

[273] Lister, S. A., & Katrina, H. (2005). The public health and medical response. CRS Report for Congress.

[274] 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.

[275] Benaioh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. In ACM CCSW '09, pp 103-114. ACM.

[276] Ibraimi, L., Asim, M., & Petkovic, M. (2009). Secure management of personal health records by applying attribute-based encryption.

[277] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., & Jonker, W. (2009). Mediated ciphertext-policy attribute-based encryption and its application. WISA.

[278] Narayan, S., Gagne, M., & Safavi-Naini, R. (2010). Privacy preserving EHR system using attribute-based infrastructure. ACM CCSW.

[279] Benaioh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. ACM CCSW '09, pp 103- 114. ACM.

[280] Atallah, M. K., Blanton, M., Fazio, N., & Frikken, K. B. (2009). Dynamic and efficient key management for access hierarchies. ACM Trans. Information System. Security., 12 (3):1-43.

[281] Benaloh, J. (2009). Key compression and its application to digital fingerprinting. Technical Report Technical Report, Microsoft Research.

[282] Blaze, M. (1993). A cryptographic file system for UNIX. In ACM Conference on Computer and Communications Security, pages 158-165.

[283] Boneh, D., Crescenzo, G. D., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. EUROCRYPT, 506 -522.

[284] ISO/TC-215 (2005). Health informatics – Electronic health record – Definition, scope, and context. Published Standard ISO/TR 20514:2005. In: International Organization for Standardization; 33.

[285] Bakker, A. (2004). Access to EHR and access control at a moment in the past: A discussion of the need and an exploration of the consequences. Int J Med Inform. 73:267-270.

[286] Hayrinena, K., Sarantoa, K., & Nykanenb, P. (2008). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. Int J Med Inform. 77, 291-304.

[287] Katehakis, D. G. (2006). Electronic health record. In: Akay M, ed. Encyclopedia of biomedical engineering. New York: John Wiley & Sons;1-8.

[288] 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. J AmMed Inform Assoc.14:1-9.

[289] Coiera, E. (2003). A guide to health informatics. 2nd ed. London: Arnold.

[290] Tang, P. C., Coye, M. J., & Bakken, S. (2003). Key capabilities of an electronic health record system: Letter report. Safety CoDSfP, ed. Washington: Institute of Medicine of the National Academies; 36.

[291] Blobel, B. (2006). Advanced and secure architectural EHR approaches. Int J Med Inform.75:185-190.

[292] Alsaker, M. & Aksnes, B. (2002). Information security in electronic health records, Kompetansesenter for IT i helsevesenet AS, Rapport, R 11/02.

[293] Gritzalis, D. (1997). A baseline security policy for distributed health care information systems, Journal of Computers & Security, 16(8), 709-719.

[294] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models, IEEE Computer 29(2), 38-47.

[295] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control, ACM Transactions on Information and System Security 4(3), 224-274.

[296] Bertino, E., Bonatti, P. A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security 4(3) 191-223.

[297] Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Transactions on Information and System Security 3(2), 85-106.

[298] Mavridis, I., Georgiadis, C., Pangalos, G., & Khair, M. (2001). Access Control based on Attribute Certificates for Medical Intranet Applications, Journal of Medical Internet Research, 3(1), e9.

[299] Hansen, F., & Oleshchuk, V. (2003). SRBAC: A Spatial Role-Based Access Control Model for Mobile Systems, Submitted.

[300] U.S. Department of Health & Human Services (2000). HIPAA Privacy Rule Summary, [online] Available at: <http://www.hhs.gov/ocr/privacy/hipaa/ understanding/summary/index.html> [Accessed 15 November 2018].

[301] Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. Communications of the ACM, vol. 53 Issue 3. 126-131.

[302] Dillema, F., & Lupetti, S. (2007). Rendezvous-based access control for medical records in the pre hospital environment. In HealthNet Proceedings of the first ACM SIGMOBILE International Workshop on Systems and Networking Support for Health care and Assisted Living Environments, (San Juan, Puerto Rico), ACM New York, NY.

[303] MHV (2010). Microsoft Health Vault. [Online] Available at: <http://www.healthvault.com/Personal/index.html> [Accessed 12 January 2019].

[304] MAK (2008). The Medical Alert Key. [Online] Available at: <http://www.healthcentral.com/migraine/reviews-202629-5.html> [Accessed 5 December 2016].

[305] Hinkamp, T. (2007). System providing medical personnel with immediate critical data for emergency treatments. Patient Application Publication 11/510, 317.

[306] Kulkarni, S., & Agrawal, R. (2008). Smartphone driven health care system for rural communities in developing countries. In HealthNet Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, Breckenridge, Colorado,, ACM New York, NY.

[307] Akinyele, J., Pagano, M., Green, M., Lehmann, C., Peterson, Z., & Rubin, A. (2009). Securing electronic medical records on smart phone. SPIMACS '09 Proceedings of the 1st ACM workshop on Security and privacy in medical and home-care systems, Hyatt Regency Chicago, IL, ACM New York, NY.

[308] Eysenbach, G. (2001). What is e-health? Journal of Medical Internet Research, 3(2), 1-20.

[309] National E-Health Transition Authority. (2011). Draft concept of operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system.

[310] Grefenstette, G. (2012). Privacy oriented access control for electronic health records. Presented in 21st International Conference on Data Usage Management on the Web Workshop at the Worldwide Web, Lyon, France.

[311] Muhammad, I., Zwicker, M., & Wickramasinghe, N. (2013). Using ANT to understand key issues for successful e-Health solutions. Proceedings of the 46th Hawaii International Conference on System Sciences, pp. 335-342.

[312] Wu, R. (2016). Secure sharing of electronic health records in clouds. Proceedings of the 8th International Conference of Collaborative Computing: Networking, Applications and Work sharing, Collaborate Com, pp. 711-718.

[313] Petkovic, M., & Ibraimi, M. (2011). Privacy and security in e-Health applications. Published in E-Health, assistive technologies and applications for assistive living: challenges and solutions, pp. 23-48.

[314] Xanthidis,D., & Aleisa, E. (2012). eHealth record and personal privacy. Proceedings of the International Conference on Information Technology and e-Services, (ISITeS), pp. 1-8.

[315] Rognehaugh, R. (1999). The health information technology dictionary. Gaithersburg, MD: Aspen. pp. 125.

[316] Rinehart-Thompson, L.A., & Harman, L.B. (2006). Privacy and confidentiality. In L.B. Harman (Ed.) Ethical Challenges in the Management of Health Information. 2, 53.

[317] Klitzman, R. (2006). The quest for privacy can make us thieves, New York Times.

[318] Ding, Y., & Klein, K. (2010). Model-driven application-level encryption for the privacy of E-health data. International Conference on Availability, Reliability, and Security, ARES, pp. 341-346.

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

[320] Jin, J., Ahn, G., Hu, H., Covington, M.J., & Zhang, X. (2009). Patient-centric authorization framework for sharing electronic health records. Proceedings of the 14th ACM symposium on Access control models and technologies, ACM SACMAT, pp. 125–134.

[321] Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. Proceedings of the 6th International ICST Conference, Secure Comm, Singapore, pp. 89–106.

[322] VanderHaak, M., Wol, A.C., Brandner, R., Drings, P., Wannenmacher, M. & Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. International Journal of Medical Informatics, 70(2-3), 117-130.

[323] Ateniese, G., Curtmola, R., de Medeiros, B., & Davis, D. (2002). Medical information privacy assurance: Cryptographic and system aspects. Proceedings of the 3rd International Conference on Security in Communication Network, SCN Amalfi, Italy, pp. 199-218.

[324] Layouni, M., Verslype, K., Sandikkaya, M.T., De Decker, B., & Vangheluwe, H. (2009). Privacy-preserving tele monitoring for eHealth. Proceedings of the 23rd Annual IFIP Working Conference on Data and Applications Security, vol 5645 of LNCS. pp. 95-110.

[325] Royle, R., Hambleton, S., Walduck, A. (2013). Review of the Personally Controlled Electronic Health Record, Australian Government, Canberra.

[326] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014), Guide to Attribute Based Access Control (ABAC) Definition and Considerations, National Institute of Standards and Technology, United States, NIST Special Publication 800-162.

[327] Macaulay, T. (2017), Understanding and Managing Risks and the Internet of Things, RioT Control, pages 279 -368.

[328] Motta, G. H . M . B., & Furuie, S. S. (2003), 'A contextual role-based access control authorization model for electronic patient records ', IEEE Information Technology in Biomedicine, vol . 7,no. l , pp. 202- 207.

[329] Dorda, W., Duftschmid, G., Gerhold, L., Gall, W., & Gambal, J. (2008), Austria's path toward nationwide electronic health records. Methods of information in medicine. 47(2):117-23

[330] Borycki, E, Joe, R. S., Armstrong, B., Bellwood, P., Campbell, R. (2011), Educating Health Professionals about the Electronic Health Record (EHR): Removing the Barriers to Adoption. Knowledge Management & E-Learning. 3 (1).

[331] Hodge, T. (2011). National Electronic Health Record Initiatives – the 2011 Who's Who.

[332] Deutsch, E., Duftschmid, G., & Dorda, W. (2010). Critical areas of national electronic health record programs-is our focus correct? Int J Med Inform. 79(3):211-22.

[333] ASTM (2000). Standard Guide for Content and Structure of the Electronic Health Record: ASTM EMR. Annual Book of ASTM Standards. 14.

[334] Ghazvini, A., & Shukur, Z. (2013). Security Challenges and Success Factors of Electronic Health care System. Procedia Technology.11:212-9.

[335] VandeVelde, R., & Degoulet, P. (2003). Clinical information systems: a component-based approach: Springer Science & Business Media.

[336] ASTM (2013). Standard Practice for Content and Structure of the Electronic Health Record (EHR). ASTM international, West Conshohocken, PA.

[337] Maharaja, A. (2009). Use of the Electronic Health Record in Private Medical Practices: ProQuest.

[338] Goel, S., Dwivedi, R., & Sherry, A. (2012). Critical factors for successful implementation of E-governance programs: a case study of HUDA. Global Journal of Flexible Systems Management.13(4):233-44.

[339] Blobel, B. (2012). Editor Standards and solutions for architecture based, ontology driven and individualized pervasive health. Phealth, Proceedings of the 9th International Conference on Wearable Micro and Nano Technologies for Personalized Health, Porto, Portugal: IOS Press.

[340] Wozak, F. (2007). Medical Data Grids as a Base-Architecture for Interregional Shared Electronic Health Records. Institute for Health Information Systems, University for Health Sciences, Medical Informatics and Technology (UMIT), Doctoral thesis.

[341] Eichelberg, M., Aden, T., Riesmeier, J., Dogac, A., & Laleci, G. B. (2006). Electronic health record standards–a brief overview. Proceedings of the 4th IEEE International Conference on Information and Communications Technology ICICT: Citeseer.

[342] Spewak, S. H., & Hill, S. C. (1993), Enterprise architecture planning: developing a blueprint for data, applications and technology. QED Information Sciences, Inc.

[343] Maldonado, J. A., Costa, C. M., Moner, D., Menárguez-Tortosa, M., Boscá, D., & Giménez, J. A. M. (2012). Using the Research EHR platform to facilitate the practical application of the EHR standards. Journal of biomedical informatics. 45(4):746-62.

[344] Xu, W., Guan, Z., Cao, H., Zhang, H., Lu, M., & Li, T. (2011). Analysis and evaluation of the Electronic Health Record standard in China: A comparison with the American national standard ASTM E 1384. International Journal of Medical Informatics. 80(8):555-61.

[345] Australian Digital Health Agency (2015). Security and Authentication. Australian Government. [Online] Available at: <https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/features-of-the-my-health-record-system/security-and-authentication> [Accessed 08 February 2019].

[346] Office of the Australian Information Commissioner (2018). Handling personal information in the My Health Record system. Privacy business resource 23. Australian government, 1 -7.

[347] Kemp, K., Arnold, B. B., & Vaile, D. (2018). My Health Record: the case for opting out. The conversation. [Online] Available at: <http://theconversation.com/my-health-record-the-case-for-opting-out-99302>. [Accessed 9 February 2019].

[348] Australian Privacy Foundation (2018). MEDIA RELEASE: 'Open Data': Too much sharing, too little care? Who's reading your health information now?. [Online] Available at: <https://privacy.org.au/2018/01/07/media-release-open-data-too-much-sharing-too-little-care-whos-reading-your-health-information-now/>. [Accessed 09 February 2019].

[349] Conrick, M., & Newell, C. (2006). Issues of Ethics and Law. In M. Conrick (Ed.), Health Informatics: Transforming Health care with Technology. Melbourne: Thomson Social Science Press.

[350] Muncaster, P. (2009). ISF releases report on cloud computing security. Itnews. [Online] Available at: < https://www.itnews.com.au/news/isf-releases-report-on-cloud-computing-security-160449>. [Accessed 10 February 2019].

[351] Duo Security Mobile (2015). Guide to Two-Factor Authentication [online] Available at: <https://guide.duosecurity.com/iphone> [Accessed February 20, 2018].

[352] Watts, J. M., & Chaturvedi, S. (2018). Singapore Health Database Hit by Cyberattack, The Wall Street Journal. [Online] Available at:

<https://www.wsj.com/articles /singapore-health-database-hit-by-cyberattack-1532085919> [Accessed 27 July 2019].

[353] Vimalachandran, P., Wang, H., Zhang Y., Cao J., Sun L., & Yong, J. (2018). Preserving Data Privacy and Security in Australian My Health Record System: A Quality Health Care Implication. Preserving Data Privacy and Security in Australian My Health Record System: A Quality Health Care Implication: 19th International Conference, Dubai, United Arab Emirates, Proceedings, Part II. 111-120.

[354] Vimalachandran, P., Wang, W., Zhang, Y., Heyward, B., & Zhao, Y. (2017). Preserving Patient-centred Controls in Electronic Health Record Systems: A Reliance-based Model Implication. International Conference on Orange Technologies ICOT. Melbourne, Australia.

[355] Vimalachandran, P., Wang, W., Zhang, Y., Heyward, B., & Whittaker, F. (2018). Ensuring Data Integrity in Electronic Health Records: A Quality Health Care Implication. International Conference on Orange Technologies ICOT. CoRR abs/1802.00577.