AN ACCESS CONTROL MODEL FOR A SOUTH AFRICAN NATIONAL ELECTRONIC HEALTH RECORD SYSTEM

by

Tamir Asrat Tsegaye

AN ACCESS CONTROL MODEL FOR A SOUTH AFRICAN NATIONAL ELECTRONIC HEALTH RECORD SYSTEM

by

Tamir Asrat Tsegaye
15T0016

Thesis

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

in the

Faculty of Commerce

of

Rhodes University

Supervisor: **Prof. Stephen Flowerday**
Co-supervisor: **Prof. Graham Wright**

December 2018

ABSTRACT

Countries such as South Africa have attempted to leverage eHealth by digitising patients' medical records with the ultimate goal of improving the delivery of healthcare. This involves the use of the Electronic Health Record (EHR) which is a longitudinal electronic record of a patient's information. The EHR is comprised of all of the encounters that have been made at different health facilities. In the national context, the EHR is also known as a national EHR which enables the sharing of patient information between points of care. Despite this, the realisation of a national EHR system puts patients' EHRs at risk. This is because patients' information, which was once only available at local health facilities in the form of paper-based records, can be accessed anywhere within the country as a national EHR. This results in security and privacy issues since patients' EHRs are shared with an increasing number of parties who are geographically distributed. This study proposes an access control model that will address the security and privacy issues by providing the right level of secure access to authorised clinicians. The proposed model is based on a combination of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). The study found that RBAC is the most common access control model that is used within the healthcare domain where users' job functions are based on roles. While RBAC is not able to handle dynamic events such as emergencies, the proposed model's use of ABAC addresses this limitation. The development of the proposed model followed the design science research paradigm and was informed by the results of the content analysis plus an expert review. The content analysis sample was retrieved by conducting a systematic literature review and the analysis of this sample resulted in 6743 tags. The proposed model was evaluated using an evaluation framework via an expert review.

DECLARATION

I declare that the thesis entitled, An Access Control Model for a South African National Electronic Health Record System, which I hereby submit for the degree, Master of Commerce at Rhodes University, is my own work. I also declare that this thesis has not previously been submitted by me for a degree at this or any other tertiary institution and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

T Tsegaye

Tamir Asrat Tsegaye

ACKNOWLEDGEMENTS

Firstly, I would like to thank my supervisor, Professor Stephen Flowerday, for his guidance, encouragement and support. The valuable advice which he provided contributed towards this thesis. I acknowledge the constructive feedback that I received from Professor Graham Wright which assisted the study.

I would like to thank my family for their support throughout the completion of this thesis.

I am also grateful for the expert reviewers who participated in this study and made a positive contribution.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

DEFINITION OF TERMS

- **Access Control:** a policy or procedure that restricts access to a system (Khan, 2012).
- **Attribute-Based Access Control:** an access control model that uses the attributes of users and objects in order to make access control decisions (Sifou, Hammouch, & Kartit, 2017).
- **Electronic Health Record:** a longitudinal electronic record of a patient's information which consists of one or more encounters in any health facility (Deloitte, 2015).
- **Electronic Medical Record:** an electronic record of an episode of medical care within a single health facility (CSIR & Department of Health, 2014).
- **Health Information Exchange:** the electronic sharing of health information between health information systems (Broyles, Dixon, Crichton, Biondich, & Grannis, 2016).
- **Health Service Bus:** middleware which facilitates interoperability by enabling disparate health information systems to communicate with each other (Hammami, Bellaaj, & Kacem, 2014).
- **Interoperability:** the extent to which two or more systems can exchange information and interpret the exchanged information (Kush, 2012).
- **One-Time Password:** a password that is valid for a single authentication session (Rayes, 2011).
- **Role-Based Access Control:** an access control model where access to certain information is granted based on the user's role (Furnell, Katsikas, Lopez, & Patel, 2008).
- **Separation of Duties:** a control that is used to prevent users from exceeding their position's level of authority (INCITS, 2012a).
- **Single Sign-On:** a mechanism that allows a user to log into an application once and allows the user to seamlessly access other applications without having to re-enter their credentials (Heckle & Lutters, 2011).

ACRONYMS

- **ABAC:** Attribute-Based Access Control
- **ANSI:** American National Standards Institute
- **CDI:** Constrained Data Item
- **DAC:** Discretionary Access Control
- **DSD**: Dynamic Separation of Duties
- **EHR:** Electronic Health Record
- **EMR:** Electronic Medical Record
- **HIE:** Health Information Exchange
- **HL7:** Health Level Seven
- **HSB:** Health Service Bus
- **IAAA:** Identification, Authentication, Authorisation and Accountability
- **INCITS:** International Committee for Information Technology Standards
- **MAC:** Mandatory Access Control
- **OTP:** One-Time Password
- **PHR:** Personal Health Record
- **PMI:** Patient Master Index
- **PoPI:** Protection of Personal Information
- **PRISMA:** Preferred Reporting Items for Systematic Reviews and Meta-Analyses
- **RBAC:** Role-Based Access Control
- **SSO:** Single Sign-On
- **TP:** Transformation Procedure
- **UDI:** Unconstrained Data Item

CHAPTER 1: INTRODUCTION

1.1. Background

Many countries have taken advantage of eHealth through the use of Information and Communications Technology (ICT) in order to improve the delivery of healthcare (Department of Health South Africa, 2012). Countries including Canada, New Zealand, Sweden and England are at different stages of implementing a national Electronic Health Record (EHR) system. A lot can be learnt from these implementations which can aid South Africa in its pursuit of having its own national EHR system.

An EHR is defined as being a longitudinal electronic record of a patient's health information, which in a national context is referred to as a national EHR (Deloitte, 2015). The EHR is longitudinal since it encompasses all the health information which is created and stored with each visit made to a hospital by the patient. This leads to benefits such as the sharing of patient information between points of care (Department of Health South Africa, 2012). This means that a patient whose EHR was updated in Region A can also be accessed in Region B, provided that both Region A and B are in the same country. Other benefits of the EHR includes monitoring diseases, a decrease in medical errors and reduced costs through avoiding redundant tests and medication (Ohuabunwa, Sun, Jean Jubanyik, & Wallis, 2016).

Although the longitudinal characteristic of the EHR has its benefits, it does have security and privacy implications. If these are not addressed effectively, this can result in the compromise of a patient's EHR leading to a loss in patient trust in the national EHR system (Alhaqbani & Fidge, 2007). Thus, it is crucial that the EHR is secured in order to prevent unauthorised access. This is made possible through the use of access control, which is used to limit access to the patient’s EHR by providing the right level of access (Whitman & Mattord, 2016). For instance, parties consisting of physicians, nurses and radiologists will each have a different level of access to a patient’s EHR. However, there are certain events which may require a party to have more access than they are currently allowed. For example, in an emergency, a patient may be unconscious and this would require the physician, who is working in the emergency department, to access the patient's EHR in order to effectively treat the patient. It is important that access which overrides enforced access control policies is audited in order to attribute any action back to the source. Accountability i.e. auditing is a fundamental part of access control which will be discussed later in Section 1.6.3. In addition to accountability, access control should also ensure the confidentiality and integrity of the EHR. This would ensure that certain patient information contained in the EHR is not disclosed to unauthorised entities (confidentiality) as well as ensuring that only authorised clinicians can modify the EHR (integrity) (Gregg, 2017). The theoretical foundation of this study, which is presented in Section 1.6.3, focuses on addressing the security and privacy issues from the research problem by ensuring the confidentiality and integrity of the EHR.

In addition to ensuring a secure and privacy compliant health information system, interoperability is needed to realise a national EHR system. This would ensure that the interoperability of health information systems would be possible at a national level. Access control and interoperability are linked: without interoperability, access control cannot be enforced on a national EHR system as this system would not exist without interoperability. Regarding a lack of interoperability, it is evident that South Africa currently faces an issue with regards to disparate systems in each of its provinces. Some provinces have health information systems which cannot communicate with other provinces, while some provinces are still paper-based (Department of Health South Africa, 2012; Ohuabunwa et al., 2016). Thus, all provinces are required to follow a common set of standards in order to ensure interoperability. The interoperability and security problems will be discussed next under the statement of the problem.

1.2. Statement of the Problem

The EHR consists of digitally stored health information which represents the patient's lifetime (Canada Health Infoway, 2006c). Consequently, since the EHR represents the patient's lifetime, it is required that the confidentiality of this information is ensured. However, a problem arises since the EHR should be shared between clinicians in order to treat the patient. As a result, confidentiality cannot be ensured since access to the patient's EHR by clinicians would violate the patient's confidentiality. Thus, access control is needed to provide the right level of secure EHR access to authorised clinicians.

In the context of South Africa, a national EHR system would also be susceptible to the security and privacy issues which would occur due to the sharing of patients' EHRs with clinicians. In addition, there has been a lack of interoperability between many South African health information systems as a result of disparate systems which cannot communicate with one another (Department of Health South Africa, 2012). Consequently, this will not allow the sharing of EHRs between authorised clinicians. This can be addressed through the realisation of an interoperable national EHR system which will enable the sharing of EHRs between authorised clinicians. However, the right level of access control will be needed in order to prevent the patient’s EHR from being compromised.

Thus, the research problem is that there is complexity involved in balancing the requirements of security, privacy and access of the EHR. The security and privacy of patients’ EHRs are at risk due to the sharing of the EHRs with an increasing number of parties. This complexity would need to be addressed through the use of access control. Additionally, by addressing interoperability, access control can be enforced on a national EHR system. The next section covers the research questions of the study.

1.3. Research Question

The main research question below has been generated from the research problem.

How should access control be enforced to realise a secure and private South African national electronic health record system?

1.3.1. Sub-Questions

The main research question has been divided into four sub-questions in order to answer the research problem.

What can South Africa learn from other countries in order to implement a secure national electronic health record system?

South Africa can learn from other countries that have implemented or are in the process of implementing a national EHR system. This would include national EHR system architectures for ensuring a secure EHR as well as lessons learned from other countries’ national EHR implementations.

What type of regulations must be followed in order for a compliant national electronic health record system to be achieved?

The national EHR system must comply with local regulations such as the Protection of Personal Information (PoPI) Act and should also follow international standards such as ISO/IEC 29100 and ISO/IEC 27001 to ensure patient privacy and security.

How can access control be used to restrict electronic health record access to authorised clinicians while also logging electronic health record access?

Access control consisting of Identification, Authentication, Authorisation and Accountability (IAAA) should be used to identify, authenticate and authorise the clinician by providing the right level of access and finally audit the actions taken by the clinician when accessing the EHR.

What is required to realise an interoperable national electronic health record system?
The national EHR system should implement interoperability standards that ensure all three levels of interoperability: foundational, syntactic and semantic interoperability in order for an interoperable national EHR system to be realised.

1.4. Objective of the Study

The objective of this study is to develop an access control model which will address the security and privacy issues which South Africa's national EHR system will face.

In order to achieve a national EHR system, interoperability challenges will also need to be addressed. This proposed model i.e. artefact was developed under the design science research paradigm, which is discussed in Section 1.7.1. In addition, an extensive literature review was conducted which comprised of the national EHR implementations of other countries, regulations, access control and interoperability standards, which informed the proposed model. Next, the significance of the study is covered.

1.5. Significance of the Study

Patient information has been identified as the most sensitive type of personal information (Canada Health Infoway, 2006a; Tipton, Forkey, & Choi, 2016). Unlike other types of personal information, it contains confidential information about the patient that cannot be changed such as the patient’s medical history. Thus, the EHR, which contains patient information, needs to be protected from unauthorised entities. The fact that many countries have embarked on realising a national EHR system puts patients’ EHRs at risk. This is because EHRs which were once only available at the local health facility will be accessed anywhere in the context of a national EHR. Hence, the security and privacy of patients' EHRs is imperative. Countries such as South Africa, which aim to have a national EHR system, will be required to secure patients' EHRs by complying with local regulations such as the PoPI Act (PoPI Act, 2013). These regulations provide requirements for the implementation of security controls such as access control which can be used to address the security and privacy risks faced by EHRs. The proposed model was developed with an emphasis on access control which is needed to ensure the security and privacy of EHRs along with regulations that inform access control. In addition to the security and privacy of EHRs, an interoperable national EHR system is essential in order for authorised clinicians to share patients' EHRs securely between disparate systems (Department of Health South Africa, 2012). As a result, better healthcare can be realised with a secure, private and interoperable national EHR system (Canada Health Infoway, 2006a). The initial review of related literature is discussed next.

1.6. Initial Literature Review

The literature review was conducted by utilising themes. These themes were categorised into four sections: national EHR adoption internationally, regulations for a compliant national EHR system, securing the EHR through access control and standards for an interoperable national EHR System. The theoretical foundation of this study is covered in Section 1.6.3. The first chapter of the literature review is summarised below.

1.6.1. National Electronic Health Record Adoption Internationally

Before a national South African EHR system can be realised, the national EHR adoption of various countries including Canada, New Zealand, Sweden and England will be examined. Each of these countries is at a different stage of their national EHR programme. The Canada Health Infoway programme comprised of developing a network of interoperable EHR solutions residing at each region (Canada Health Infoway, 2006c). This puts Canada at the regional level of an EHR. Similarly, New Zealand's EHR strategy places emphasis on a single 'physical' EHR with regional repositories which provide the foundation. However, currently in New Zealand, a virtual EHR is being used within a point-to-point model. A virtual EHR is defined as systems which assemble disparate data on demand and this combined data is displayed via interfaces and software (Deloitte, 2015). Positioned at an advanced stage of providing access to a national EHR, Sweden's disparate health information systems have been able to exchange information through the use of a national Health Information Exchange (HIE) platform (Hägglund & Scandurra, 2017). With regards to England's Summary Care Record (SCR) i.e. EHR, Parkin (2016) states that "As of February 2016, 55.06 million people have had a SCR created" (p. 3). This SCR contains patient information such as medication, allergies and adverse reactions. Each of the examined countries has experienced challenges during their national EHR implementations (as discussed in Chapter 3: Section 3.5). These challenges can serve as lessons learned for South Africa's national EHR system so that the same mistakes are not repeated. Regulations that can assist in ensuring a secure and private national EHR system are examined next.

1.6.2. Regulations for a Compliant National Electronic Health Record System

ISO/IEC 27001 (2013) states that an access control policy should be established, documented and reviewed based on organisation and information security requirements. This is imperative since the definition of an access control policy will determine how access to a patient's EHR will be controlled. On the other hand, ISO/IEC 29100 provides a privacy framework for protecting personal information, such as a patient's EHR, which could be at risk during the processing of personal information (ISO/IEC 29100, 2011). Thus, ISO/IEC 29100 is aligned with regulations such as the PoPI Act since it also focuses on the processing of personal information. The PoPI Act, which was enacted in South Africa in 2013, is a regulation that emphasises the protection of personal information which is processed by public and private bodies (PoPI Act, 2013). Both public and private hospitals that will be part of the national EHR system would need to comply with the PoPI Act. Implementing an access control policy which would safeguard patients' personal information through the use of access control, would aid compliance with the PoPI Act. Access control needed to secure the EHR is discussed below.

1.6.3. Securing the Electronic Health Record through Access Control

Access control is a policy or procedure that restricts access to a system (Khan, 2012). Access control comprises of several components: identification, authentication, authorisation and accountability. Identification involves identifying the clinician attempting to access the system. Authentication is used to verify the identity of the clinician who will then be granted a certain level of access via authorisation. Lastly, accountability is needed in order to monitor a system and record any actions that are made on the system. Additionally, in the event that a clinician accesses a patient's EHR without their permission, the accountability component would ensure that this access is recorded.

Authorisation is an essential part of the IAAA since the type and configuration of this component will determine how access control decisions will be made when a clinician accesses a patient's EHR. Four potential access control models that can be used to secure an EHR are discussed by Furnell, Katsikas, Lopez, and Patel (2008). These include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC). DAC allows the owner of a file to grant file access to new users. In the context of an EHR, a doctor who has access to a patient's EHR can grant access to a specialist whom a patient is referred to. On the other hand, in MAC access control decisions are made based on the security level (top secret > secret > confidential > unclassified) of users and files. For example, a user with the security level of ‘confidential’ would be able to access a file that has the ‘confidential’ or ‘unclassified’ security level. On the contrary, in ABAC access is granted based on the attributes of subjects and objects. For instance, by using ABAC, access to a patient’s EHR can be granted in the event of an emergency. In contrast, in RBAC access to certain information is based on the user’s role. For example, the physician role which is assigned with the append permission to a patient’s EHR will allow the physician to add notes to the EHR.

There are numerous theoretical models which ensure the confidentiality or integrity of information. Firstly, adhering to the ANSI RBAC standard ensures that access control is based on roles and not individual users (INCITS, 2012a). Additionally, the ANSI RBAC policy-enhanced standard, which is an enhancement of the ANSI RBAC standard, can also be used to handle dynamic events such as emergencies via ABAC (INCITS, 2012b). Chen, Shing, Lee, and Shing (2007) discuss the Bell-LaPadula model where a subject possesses a security clearance and an object has a security classification. The goal of this model is to ensure confidentiality by preventing read access to objects with a higher security classification than the subject’s clearance. Wu, Ahn, Hu, and Singhal (2010) discuss the Chinese wall model which also ensures the confidentiality of information. It does this by making use of subjects and objects to prevent information flows which cause a conflict of interest. In addition to the three discussed models, Byun, Sohn, and Bertino (2006) cover two models which ensure integrity: the Biba model and Clark-Wilson model. The Biba model prevents data corruption by limiting information flow among data objects. The Clark-Wilson model also ensures integrity by preventing improper data modification by enforcing mechanisms such as separation of duty and well-formed transactions. Gregg (2017) adds that the Clark-Wilson model specifies that users must access data through an application and mentions that auditing is mandatory. This is relevant to this study since access control will be part of the application and will consequently restrict access to the patient’s EHR while auditing is an essential part of access control which will be used for recording EHR access. Standards for ensuring an interoperable national EHR system are discussed below.

1.6.4. Standards for an Interoperable National Electronic Health Record System

Adhering to interoperability standards is important in order to realise an interoperable national EHR system. This would require that health information systems, which are connected together to form a national EHR system, adhere to interoperability standards. Adherence to interoperability standards should ensure all three levels of interoperability: foundational, syntactic and semantic interoperability. Broyles, Dixon, Crichton, Biondich, and Grannis (2016) discuss each level of interoperability. Foundational interoperability enables systems to exchange information over network. This level of interoperability is fundamental as it ensures that systems are connected together. On the other hand, syntactic interoperability requires that the exchanged information is in a format that is recognised by the communicating systems. However, syntactic interoperability does not enable the receiving system to interpret the information. This is addressed by semantic interoperability which ensures that the communicating systems can interpret the received information. Hence, in order for interoperability to be realised, the national EHR system would need to achieve all three levels of interoperability.

In summary, Section 1.6.1 discussed a number of countries and the current stage that they are in with regards to implementing a national EHR system. Section 1.6.2 covered regulations which are needed to enforce access control along with standards which can be used as a guide when complying with regulations. Next, Section 1.6.3 covered four access control models. In addition, six theoretical models were also covered which are based on the examined access control models. Out of these six theoretical models, three will be used as the theoretical foundation of this study: the ANSI RBAC standard, ANSI RBAC policy-enhanced standard and the Clark-Wilson model. The ANSI RBAC standard was selected since access control decisions can be made based on clinicians' roles. The ANSI RBAC policy-enhanced standard was also selected since it addresses RBAC's limitation of not supporting dynamic events such emergencies. The Clark-Wilson model was chosen since its concepts, such as auditing, separation of duties and well-formed transactions, can be applied to the new context of a national EHR system. Finally, Section 1.6.4 examined interoperability which is needed in order to realise an interoperable national EHR system. The research design comprising of research paradigm and methods is discussed below.

1.7. Research Design

This section introduces the design science research paradigm which was followed by this study. Additionally, the research methods, including a content analysis and expert review, are also covered which includes a discussion of the data collection and analysis methods which were used in this research study. The design science research paradigm, which served as a basis for the development of the proposed model, is discussed next.

1.7.1. Research Paradigm

The research paradigm followed in this study is design science. Design science addresses a research problem by creating and evaluating an artefact designed to meet an identified need (Hevner, March, Park, & Ram, 2004). The design science research paradigm was chosen for this research study since the creation of the proposed model i.e. artefact was appropriate for addressing the research problem. In design science, artefacts are defined as constructs, models, methods or instantiations (Hevner et al., 2004). Models assist problem and solution understanding and frequently represent the connection between problem and solution components. The creation of a model was the focus of this study. This study followed the seven design science research guidelines proposed by Hevner et al. (2004) when creating the proposed model. The seven design science research guidelines are available in Chapter 2: Table 2.2. Next, the research methods, which were used by the study, are covered.

1.7.2. Research Methods

The research methods which were used in this study included a content analysis and expert review. The content analysis method was selected since it was able to quantify the qualitative literature which resulted in tagged codes in the area of access control and the EHR. An expert review, consisting of security and health experts, was also conducted to evaluate the credibility of the proposed model which resulted in feedback. The expert review was selected since it meets design science research guideline 3 (which is discussed in Chapter 2: Section 2.3.4.2). In addition, the proposed model was also informed by conducting an extensive literature review using critical thought. The results of the content analysis, expert review and critical thinking informed the proposed model which indicated that the proposed model was triangulated and was informed by multiple research methods, thus increasing the validity of the study. The study followed a mixed methods approach in order to triangulate the proposed model. The selected research methods are discussed in more detail in Chapter 2: Section 2.5. The delimitation of the study is discussed below.

1.8. Delimitation of the Study

The scope of this study focuses on the access control part of EHRs. The low-level details regarding how the national EHR is created are not covered. In addition, the study focusses on logical access control. Standards that ensure the security and privacy of EHRs are included along with healthcare interoperability standards for ensuring an interoperable national EHR system. Standards that focus on the usability of the EHR i.e. usability standards are not covered by this study. This study does not focus on the costs of national EHR systems. Health insurance and medical aid companies are not included in the scope of this study. Ethical considerations applicable to this study are covered in the next section.

1.9. Ethical Considerations

This study abided by a number of principles for ethical conduct in research including honesty, openness, respect for intellectual property and confidentiality (Shamoo & Resnik, 2015). The communications of the study were honestly reported. This included the honest reporting of methods used, results and publications. The principle of openness was also followed when receiving feedback from the expert review. Respect for intellectual property was ensured by acknowledging the research contributions made by others. The confidentiality of the expert reviewers, who participated in the study, was preserved by ensuring that they remained anonymous. Ethical clearance was obtained from the Rhodes University Ethics Committee (ethical approval number: CIS18-03) before the selected expert reviewers were invited to take part in the study. An overview of the proposed model, which is the contribution of this study, is covered below.

1.10. Contribution: Proposed Model

The proposed model, illustrated in Figure 1.1, was created to address the research problem which was discussed in Section 1.2. This is achieved through the use of access control which controls access to the national EHR. This ensures that only authorised clinicians have access to the patient's EHR while also ensuring that clinicians only have access to patient information which they require to perform their job function. The manner in which access control limits access to the patient's EHR is informed by the study's theoretical foundation, which was introduced in Section 1.6.3. As a result, access control decisions are made based on the role of the clinician using RBAC while EHR access can be granted in an emergency via ABAC. Since the proposed model also includes the accountability component of access control, exceptional access in the event of an emergency is audited. This ensures that clinicians are held accountable for any misuse of patient information. While the main focus of the proposed model is on the security and privacy aspects of the research problem, it also addresses the interoperability issues which would arise due to the use of disparate systems in different regions. Interoperability is an important aspect of a national EHR system since without interoperability, access control cannot be enforced on a national EHR system which can only exist if interoperability between regional health information systems is realised. The justification of

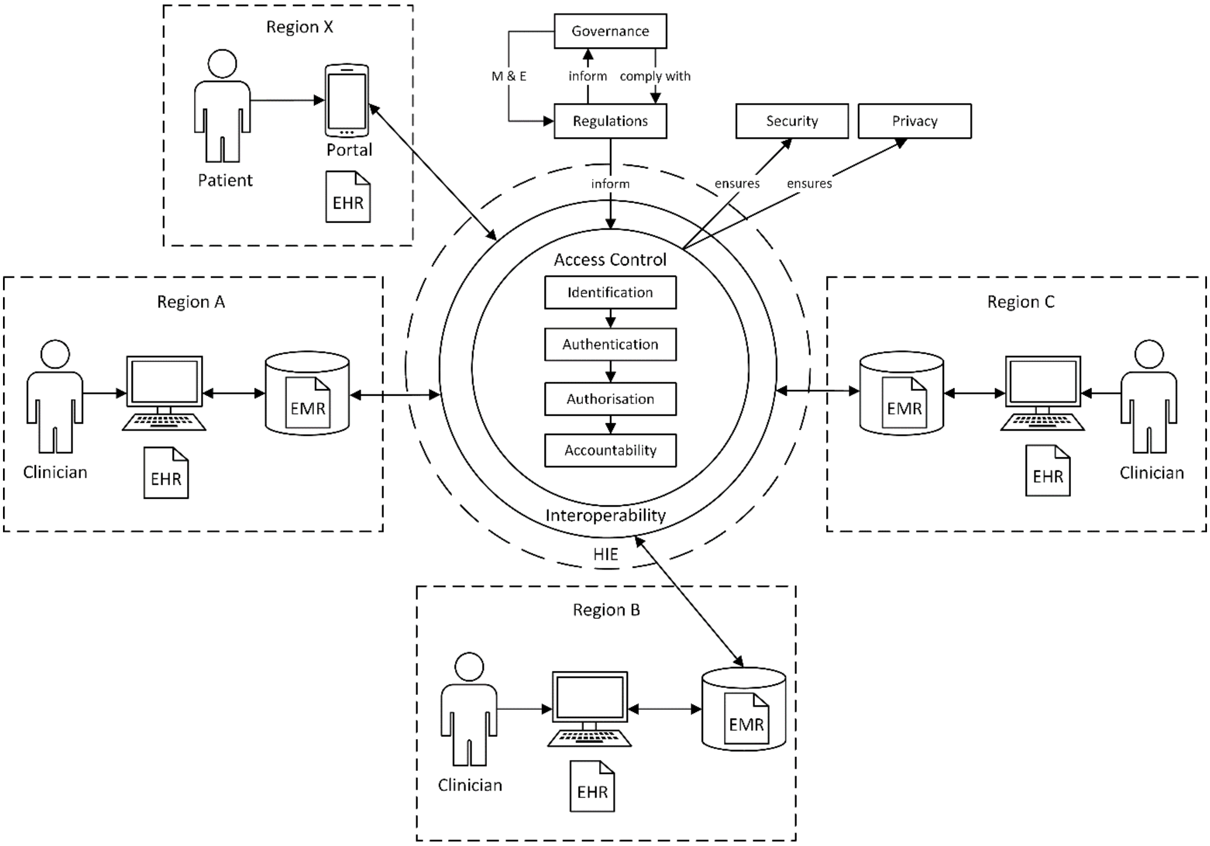


Figure 1.1: Proposed access control model

the key components which were included in the proposed model are covered in Chapter 8: Section 8.5. Chapter 8: Section 8.6 covers the proposed model in more detail by focussing on each of its key components. The next section outlines the chapters of this research study.

1.11. Outline of Chapters

The outline of the chapters is illustrated in Figure 1.2. Chapter 1 introduced the reader to the background of the study followed by the statement of the problem which this research study addresses. The research question, which is divided into four sub-questions, was then covered along with the objectives and significance of the study. This was followed by an introductory literature review in the area of access control and EHRs. Next, the research design, comprising of the research paradigm and research methods, was introduced. Chapter 1 ended with the delimitation of the study and ethical considerations. Chapter 2 discusses the extended research design and methods including the content analysis and expert review which informed the proposed model. An extended literature review is covered over Chapters 3, 4, 5 and 6. Chapter 3 discusses the national EHR adoption internationally. Chapter 4 covers the regulations needed for a compliant national EHR system. Chapter 5 covers securing the EHR with access control. Chapter 6 examines standards for an interoperable national EHR system. Next, Chapter 7 discusses the findings and analysis of the study and Chapter 8 covers the recommendations and proposed model. Finally, the study is concluded in Chapter 9.

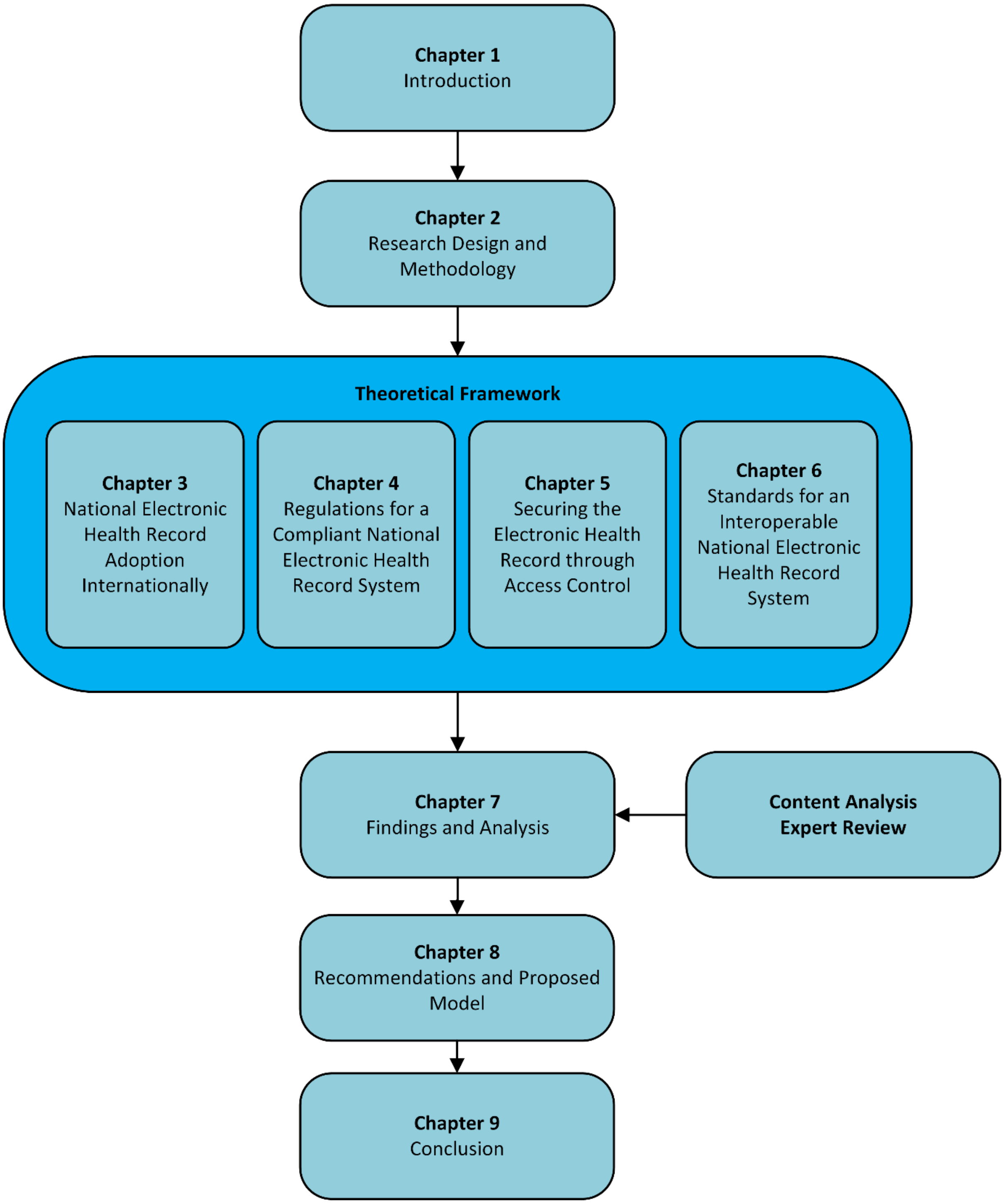

Chapter 1
Introduction
Chapter 2
Research Design and Methodology
Theoretical Framework
Chapter 3
National Electronic Health Record Adoption Internationally
Chapter 4
Regulations for a Compliant National Electronic Health Record System
Chapter 5
Securing the Electronic Health Record through Access Control
Chapter 6
Standards for an Interoperable National Electronic Health Record System
Chapter 7
Findings and Analysis
Content Analysis
Expert Review
Chapter 8
Recommendations and Proposed Model
Chapter 9
Conclusion

Figure 1.2: Outline of chapters

CHAPTER 2: RESEARCH DESIGN AND METHODOLOGY

2.1. Introduction

This chapter sets out to explain the research design and methodology used in this study. The research design and methodology which were followed were influenced by the research problem of balancing the requirements of the security, privacy and access of the EHR. The discussion begins with examining the research design and methodology structure which highlights the different layers of this structure. Next, a number of key research paradigms are compared and the chosen paradigm is justified as this paradigm determined how the research was conducted. The different types of research methods are also discussed along with the data collection and analysis methods which were determined by the selected research method. Lastly, the ethical considerations which were applicable to the study are highlighted. The structure of the research design and methodology, which were used in this study, are discussed below.

2.2. Research Design and Methodology Structure

The structure of this research design and methodology chapter will be discussed with regards to the research onion. Saunders, Lewis, and Thornhill (2009) discuss the research onion in terms of the various elements of the research process which this research onion represents. These elements are represented as layers and a core as illustrated in Figure 2.1. The elements which are used in this study are circled in the red. The research process starts at the outermost layer which focuses on research philosophies or paradigms. The selected research paradigm will determine how the researcher views the world and which methods will be chosen for the study. Thus, the researcher should not start with the centre of the research onion (data collection and analysis) but should start with the outermost layer. It is the outermost layer that will determine the type of data collection and analysis methods that will be chosen. The research philosophy that was selected for this study was design science. The next layer is the approaches layer, which consists of the deductive and inductive approaches. The deductive approach comprises of placing a theory under a rigorous test. On the other hand, in the inductive approach the data would first be collected after which a theory would be developed (Creswell, 2014). In terms of this study, an inductive approach was followed. The next layer, which is research strategies, is not covered in this study along with the time horizons layer. The following layer is the choices layer and in the context of this study, mixed methods was selected. Finally, the core of the research onion represents techniques and procedures

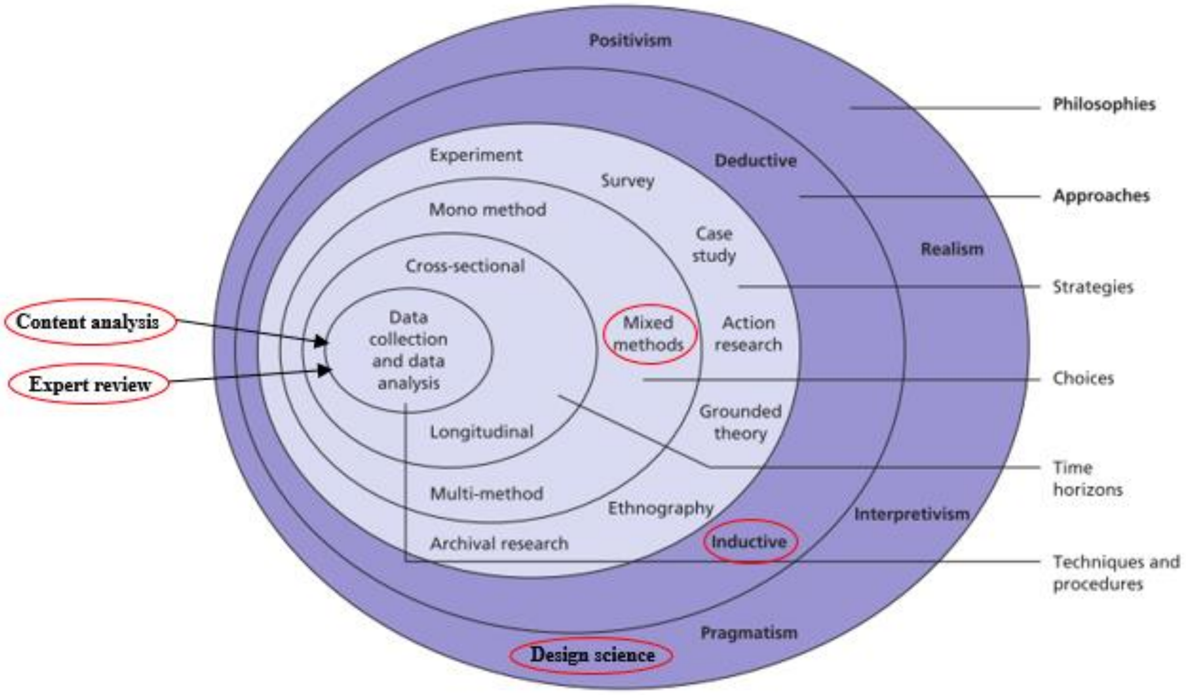


Figure 2.1: Research onion – adapted from Saunders et al. (2009)

comprising of data collection and analysis methods. Since this study is based on mixed methods, it used a combination of qualitative and quantitative methods with more emphasis being placed on the qualitative approach. For instance, the MAXQDA software programme was used to quantify the qualitative literature while the expert review feedback was analysed qualitatively using narration. The next section compares the various research paradigms which is followed by a more thorough discussion of the selected research paradigm for this study: design science.

2.3. Research Paradigms

The type of research paradigm that is selected is significant as it will determine how the research is conducted. Wahyuni (2012) states that a research paradigm consists of important assumptions and beliefs where the world is perceived and the chosen research paradigm will guide the researcher's behaviour. The research paradigm that the researcher chooses will be unique in terms of its ontology, epistemology, axiology and methodology. Vaishnavi and Kuechler (2015) state that ontology is the study which defines the nature of reality e.g. what is real and what is not. On the other hand, epistemology is the study which focuses on the nature of knowledge e.g. what does the knowledge depend on and how can one be certain of what they know. Axiology is defined as the study of values. It focuses on the values which are held by the researcher and the reason why those values are chosen. Lastly, the methodology is also

Table 2.1 Comparison of research paradigms in terms of philosophical assumptions – adapted from (Creswell, 2014; Goldkuhl, 2012; Saunders et al., 2009; Tsang, 2014; Vaishnavi & Kuechler, 2015; Wahyuni, 2012)

	Research Paradigms			
Assumptions	Positivism	Interpretivism	Pragmatism	Design Science
Ontology	Single objective reality	Multiple realities viewed as being socially constructed	Based on actions in a world that is in a constant state of change	Multiple world-states
Epistemology	Discovering law-like relationships involving causation	Interpreting subjective meanings and actions of subjects	Knowledge useful for action and change	Knowing through making
Methodology	Quantitative methods such as experiments and statistical analysis	Qualitative methods such as interviews	Mixed methods	Developmental and measurement of artefact impact
Axiology	Values truth	Value bound	Values have a role in interpreting results	Values problem solving

important as it will determine if the researcher will base their study on a qualitative, quantitative or a mixed methods approach. The four research paradigms which are discussed in this chapter vary widely in terms of their ontology, epistemology, axiolgy and methodology as represented in Table 2.1. The first research paradigm, positivism, is discussed below.

2.3.1. Positivism

In positivism, reality is represented by objects that have an existence which is separate from the researcher (Saunders et al., 2009). Ontologically, this reality is represented as a single objective reality which is the same for everyone irrespective of their values. Thus, the data that is collected by the researcher is objective since it is less prone to bias. Olivier (2009) elaborates on this by stating that the researcher does not influence the results and another researcher who repeats the research will end up getting the same results regardless of their personal characteristics. On the other hand, Saunders et al. (2009) state that some may argue that it is impossible for the researcher to not include their values in the study. For example, the positivist can choose which problem to study, what research objectives to select and what type of data to collect. Regarding epistemology, Tsang (2014) mentions that positivists use a deductive approach with the aim of discovering law-like relationships involving causation. This achieved through the use of a structured methodology that involves the use of quantitative methods such as experiments and statistical analysis. With regards to axiology, the positivist values truth

(Vaishnavi & Kuechler, 2015). This is due to the objective nature of the positivist's study. Interpretivism, which contrasts positivism, is covered next.

2.3.2. Interpretivism

Interpretivism emphasises that researchers should understand the subjective meanings that their subjects attach to the world through interaction (Wahyuni, 2012). This is in contrast to positivism where the emphasis is on objects as opposed to people. Tsang (2014) further contrasts interpretivism with positivism by stating that interpretivism considers the methods of natural science insufficient for conducting social science research. Ontologically, this is due to interpretivists viewing multiple realities as being socially constructed and are thus subjective. Epistemologically, knowledge is created by interpreting the subjective meanings and actions of subjects according to the interpretivist's own frame of reference. Regarding ontology and epistemology, Goldkuhl (2012) states that these two assumptions are linked since knowledge, comprising of understanding and meanings, is important in the ontological assumptions of the constitution of the world. On the other hand, ontology and epistemology are separate in positivism. In interpretivism, the subjective meanings and actions of subjects are interpreted through the use of qualitative methods such as interviews (Wahyuni, 2012). The axiology of the interpretivist is also affected by subjectivity and is thus value bound. This is due to the interpretivist's research which can never be bias-free due to being influenced by the researcher's thoughts, feelings, opinions and experiences (Bunniss & Kelly, 2010). The third research paradigm, pragmatism, is examined next.

2.3.3. Pragmatism

In pragmatism, it is normal for the pragmatist to work with variations in ontology, epistemology and axiology (Saunders et al., 2009). This differs to both positivism and interpretivism where each of these research paradigms have a more rigid view on these three assumptions. Creswell (2014) adds that pragmatism is not bound to any one system of philosophy and reality. This allows the pragmatist to draw from both the positivism and interpretivism stances on ontology, epistemology and axiology. Ontology in pragmatism is based on actions and change i.e. people act in a world that is in a constant state of change (Goldkuhl, 2012). Thus, actions are fundamental to the pragmatism research paradigm. Epistemologically, the pragmatist views knowledge as being useful for action and change. This knowledge is not restricted to explanations (as is the case with positivism) and understanding (under interpretivism). Regarding the pragmatist methodology, it is evident that pragmatism draws from both positivist and interpretivist methods. Creswell (2014) mentions that pragmatists are free to choose the methods, techniques and procedures that best suit their needs. This is done through the use of mixed methods which draws from both quantitative and qualitative methods. Lastly, the axiological stance of pragmatism states that values have a role in interpreting results (Wahyuni, 2012). In addition, the pragmatist adopts both subjective and objective points of view. Design science, which is the selected research paradigm for his study, is covered below.

2.3.4. Design Science

Similar to pragmatism, design science is a research paradigm that also places an emphasis on action through the practical application of a solution. Design science does this through addressing a research problem by creating and evaluating an artefact designed to meet an identified need (Hevner et al., 2004). Vaishnavi and Kuechler (2015) discuss the beliefs of design science under ontology, epistemology, methodology and axiology. Ontologically, design science researchers believe in multiple world-states, which is in contrast to positivism where a single reality is believed. Additionally, the multiple realities of the interpretivist are not the same as the multiple world-states of the design science researcher. Regarding the epistemological stance of the design science researcher, the emphasis is on knowing through making. This is evident since design science is about developing an artefact which should result in the creation of new knowledge. The design science methodology emphasises the development of the artefact and that the impact of the artefact must be measureable. The measurement of the impact is important as it will identify what contributions the artefact will make in a specific context. In terms of axiology, design science values problem solving and improvement. This is imperative as the artefact which is produced from the problem solving process should make an improvement to the applied context.

Thus, the design science paradigm has been chosen for this study since the creation of an artefact is appropriate for addressing the research problem within the context of a national EHR system. In design science, artefacts are defined as constructs, models, methods or instantiations (Hevner et al., 2004). Models assist problem and solution understanding and frequently represent the connection between problem and solution components. The creation of a model was the focus of this study. Figure 2.2 depicts an artefact which interacts with a context (Wieringa, 2014). This artefact can be a method, technique, conceptual structure, etc. In terms of this study, the artefact is the conceptual structure i.e. model. On the other hand, the context is made up of various components. In the context of a national EHR system, this is comprised of more than one component such as the software, hardware, people, etc. Figure 2.2 illustrates that the artefact cannot solve a problem by itself. It is the interaction between the artefact and context which contributes to solving the problem. This problem has a context in which the aim is improvement and in order to understand the problem the context must be understood.

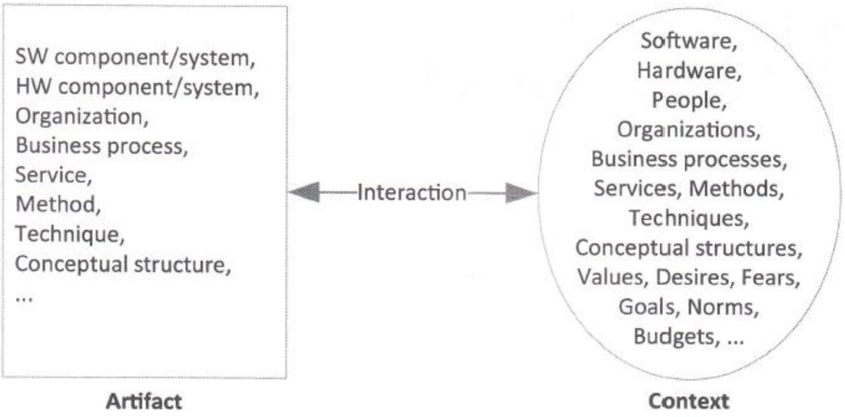


Figure 2.2: An artefact interacting with a context (Wieringa, 2014)

Gregor and Hevner (2013) discuss a design science research knowledge contribution framework which is used to identify the different types of contributions a design science research study may make. It is represented in Figure 2.3 as a 2 x 2 matrix of research study contexts and potential design science research contributions. The focus of this study is in the

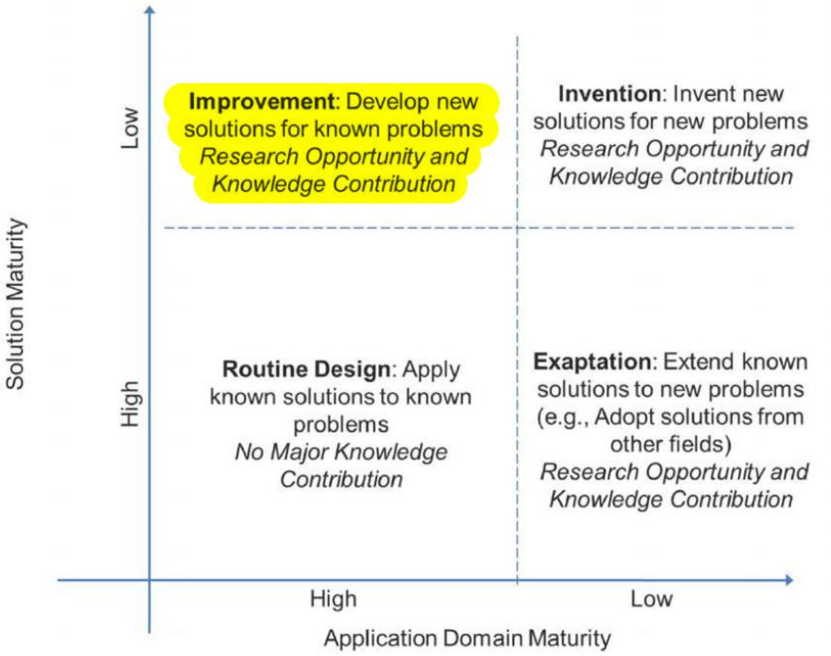

Low
High
Solution Maturity
Improvement: Develop new solutions for known problems
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems
Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
High
Low
Application Domain Maturity

Figure 2.3: Design science research knowledge contribution framework – adapted from Gregor and Hevner (2013)

improvement quadrant. Research studies in the improvement quadrant aim to develop new solutions for known problems. In order to justify this improvement, the proposed model will be compared to current solutions as well as evaluated against certain criteria. In the next section, the Information Systems (IS) research framework is discussed in terms of the design science paradigm.

2.3.4.1. *Information Systems Research Framework*

The design science paradigm, as discussed in the previous section, was chosen since the creation of an artefact is appropriate for addressing the research problem. Design science can be further explained by discussing the IS research framework which is illustrated in Figure 2.4. This is a conceptual framework, created by Hevner et al. (2004), for understanding, executing and evaluating IS research which combines the behavioural science and design science paradigms. For the purposes of this discussion, only the design science paradigm will be discussed.

In Figure 2.4, the environment defines the problem space which has a context and in this instance is the national EHR system. The environment is comprised of people, organisations and their technologies. Business needs are evaluated within the context of organisational strategies, structure, culture and business processes. This is done relative to the technology infrastructure, applications, communications architecture and development capabilities. These all define the business need i.e. problem. The research relevance is ensured by creating research activities to address the research problem.

The artefact which is developed is justified/evaluated. This will result in assessing and refining the artefact in iterations using methods such as case studies and simulations. For the purposes of this study, two methods will be used: an expert review will be conducted to evaluate the proposed model while the results of a content analysis will be used to inform the proposed model. This artefact should be applicable to a specific environment, where it should address the research problem. Furthermore, the artefact should make additions to the knowledge base. The knowledge base, which is comprised of foundations and methodologies, provides the resources from which IS research can draw from. The researcher can access foundational theories, frameworks, instruments, constructs, models, methods and instantiations which have been used in previous IS research in order to develop/build the artefact. Methodologies provide

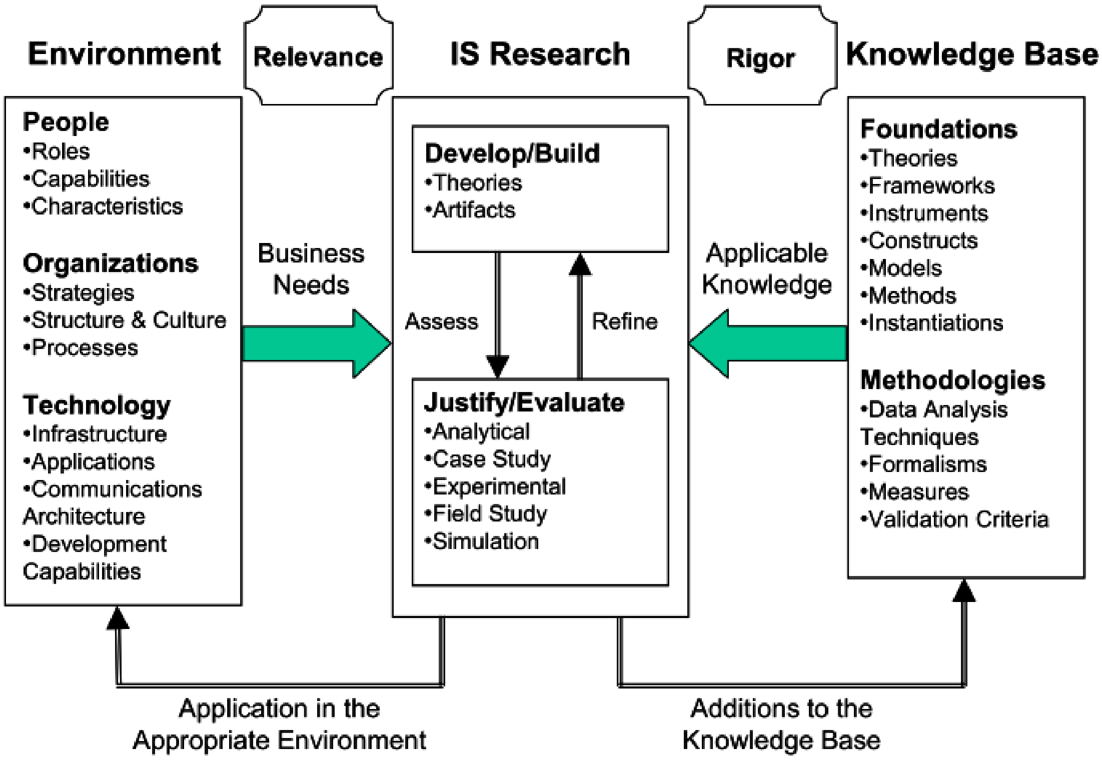


Figure 2.4: Information systems research framework (Hevner et al., 2004)

guidelines that can be used during the justify/evaluate activity. Rigour is ensured by appropriately making use of existing foundations and methodologies from the knowledge base. Next, the design science research guidelines will be discussed in terms of this study.

2.3.4.2. *Design Science Research Guidelines*

This study followed the seven design science research guidelines proposed by Hevner et al. (2004) when creating the proposed model. The seven guidelines are depicted in Table 2.2. The guidelines do not need to be addressed in order. These guidelines are discussed in more detail below in the context of this study:

- **Guideline 1: Design as an Artefact**
  The artefact that was created in this study was a model which addresses the research problem of balancing the requirements of security, privacy and access of the EHR through access control. It is applicable to the context of a South African national EHR system.

- **Guideline 2: Problem Relevance**
  The problem that was addressed by the proposed model is relevant as it pertains to allowing the sharing of sensitive patient information with authorised clinicians while

controlling access via access control. This is important since different clinicians should have different levels of access to the EHR.

- **Guideline 3: Design Evaluation**
  The proposed model was evaluated via an expert review using questions that were based on Weber's (2012) evaluation framework. Additionally, the utility, quality and efficacy of the proposed model were demonstrated by the questions in Appendix A. For example, Question 3 (access control) was aligned with utility while Question 6 (health information systems) focussed on efficacy. Thirdly, the quality of the proposed model was evaluated by using the criteria from Weber's (2012) evaluation framework (as discussed in Chapter 7: Section 7.3.1). The expert review was executed rigorously through the selection of experts from multiple disciplines: security experts and health experts (consisting of health IT experts and medical doctors). The security experts answered the access control questionnaire while the health experts answered the health information systems questionnaire. These experts provided feedback that was used to inform the proposed model.

- **Guideline 4: Research Contributions**
  Research contributions in design science consist of a design artefact, design foundations and/or design methodologies (Hevner et al., 2004). The contribution of the study was a design artefact i.e. model applicable to the context of a South African national EHR system. The aim of the study was to contribute a new solution (improvement) to a known problem.

- **Guideline 5: Research Rigour**
  Rigorous methods used in this study comprised of an extensive review of related literature using critical thought on access control and the EHR, content analysis and an expert review. The results of conducting an extensive literature review, content analysis results and expert review feedback informed the proposed model, which indicated that the proposed model was triangulated and was informed by multiple research methods. As a result, the rigour of this study was ensured.

- **Guideline 6: Design as a Search Process**

  The design of the proposed model was refined through an iterative process. This iterative process was included in some of the research methods used in this study. Literature, which was collected and later analysed, was categorised into themes in the area of access control and EHRs. Literature was also collected and analysed using content analysis and the codes generated from this process were further refined through an iterative process.

- **Guideline 7: Communication of Research**
  The findings of this study will be published in journals and a conference proceeding. This thesis will also be accessible in the library of the Rhodes University. The research methods that were used in this study are discussed next.

Table 2.2: Design science research guidelines – adapted from Hevner et al. (2004)

Guideline	Description
Guideline 1: Design as an Artefact	Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaulation methods.
Guideline 4: Research Contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5: Research Rigour	Design science research relies upon the application of rigourous methods in both the construction and evaluation of the design artefact.
Guideline 6: Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

2.4. Research Methods

There are several types of research methods that a study may use. The selected research methods will be influenced by the underlying research paradigm, which in this instance was design science. Figure 2.5 represents the research methods continuum with the three main research methods being represented on the continuum: quantitative and qualitative methods appear on opposite ends of the continuum while mixed methods appear in the middle.

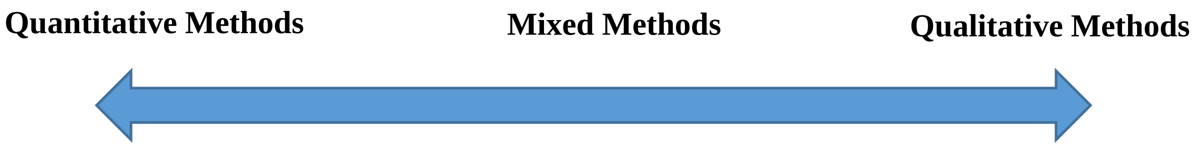


Figure 2.5: Research methods continuum - adapted from Johnson, Onwuegbuzie, and Turner (2007)

Creswell (2014) mentions that mixed methods are located in the middle of the continuum since it includes components of both quantitative and qualitative methods. Saunders et al. (2009) define ‘research choice’ as the way in which one chooses to combine quantitative and qualitative approaches. When choosing research methods, one will either use a mono method or multiple methods. A mono method comprises of using a single data collection procedure and a corresponding data analysis procedure, while multiple methods consists of using multiple data collection and analysis procedures. Multiple methods are further broken down into other subcategories as depicted in Figure 2.6 and will be discussed as they relate to this study. Firstly, quantitative research is examined below.

2.4.1. Quantitative Research

Quantitative research is defined as research that explains phenomena in terms of numeric data which is analysed using mathematical methods (Yilmaz, 2013). Saunders et al. (2009) elaborate on this by mentioning that data analysis in quantitative research can be done via statistics or graphs while data collection methods such as questionnaires can be used to collect the data using closed-ended questions. In quantitative research, the emphasis is on testing theories deductively, protecting the research against bias as well as generalising and replicating results (Creswell, 2014). Qualitative research, which is on the other end of the continuum, is discussed next.

2.4.2. Qualitative Research

Qualitative research is an approach that involves the interpretation of symbolic data obtained from subjects (Schreier, 2012). This symbolic data can consist of visual and verbal data such as pictures and audio recordings. The use of non-numeric data in qualitative research thus contrasts quantitative research where numeric data is collected. In qualitative research, data collection techniques such as interviews with open-ended questions are used while the data is analysed using methods that could include categorising the data into themes (Saunders et al., 2009). In addition, the use of an inductive approach and interpretation of meaning is important in qualitative research (Yilmaz, 2013). Lastly mixed methods research, which is in the middle of the continuum, is examined below.

2.4.3. Mixed Methods Research

Mixed methods research consists of elements of both the quantitative and qualitative approaches with the aim of corroborating results (Johnson et al., 2007). This corroboration of results is termed as triangulation where these results originate from the use of different methods which should all support the same result. In the context of this study, the result corresponds to the proposed model which was informed by the content analysis, expert review and critical thinking. The proposed model is triangulated since it has been informed by multiple research methods as illustrated in Figure 2.6. As a result, the validity of the study is increased. The results of the content analysis and expert review are discussed in Chapter 7: Sections 7.2 and 7.3 respectively, while the use of critical thinking for informing the proposed model is covered in Chapter 8: Section 8.5. Regarding the multi-method approach in Figure 2.7, although this refers to the combination of more than one data collection procedure with a corresponding analysis procedure, this does not fall under mixed methods since the multi-method approach does not allow for the mixing of quantitative and qualitative methods (Saunders et al., 2009). Conversely, mixed method and mixed-model research allow for the mixing of quantitative and qualitative methods. In mixed method research, quantitative data is analysed quantitatively while qualitative data is analysed qualitatively. Mixed-model research, which is circled in

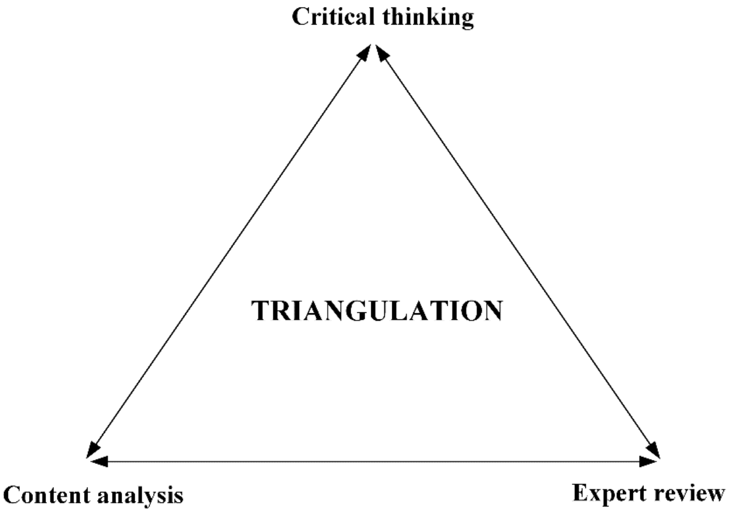


Figure 2.6: Triangulation applied to this study – adapted from Firat and Yurdakul (2011)

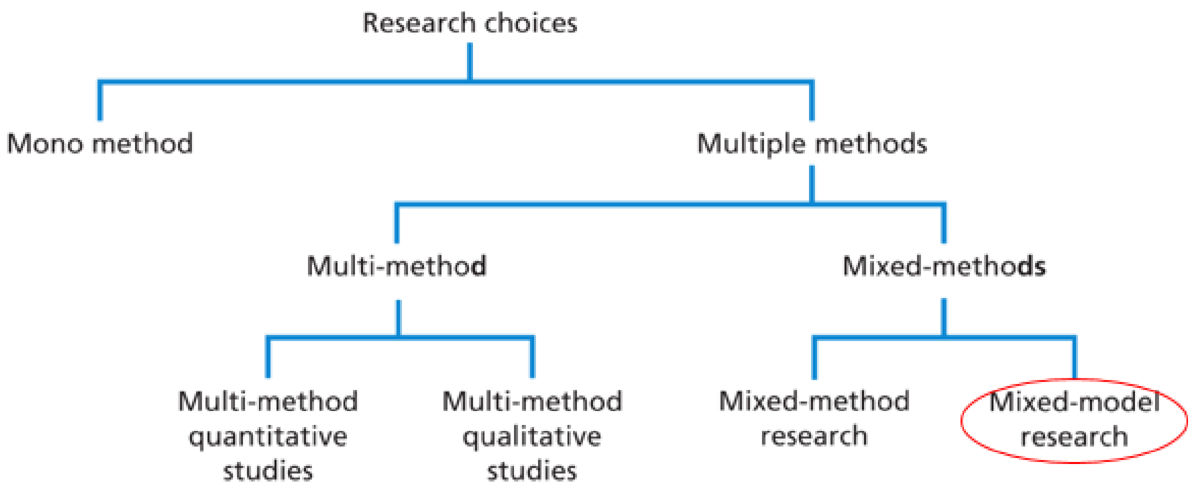


Figure 2.7: Research choices – adapted from Saunders et al. (2009)

Figure 2.7, is applicable to this study since qualitative data may be analysed quantitatively. In this case the qualitative literature was analysed quantitatively using content analysis which resulted in numeric results. On the other hand, the expert review feedback was analysed qualitatively using narration. This is discussed in more detail in the following section: data collection and analysis methods.

2.5. Data Collection and Analysis Methods

As discussed in the previous section, this study is based on mixed methods. Hence, the selected data collection and analysis methods are mostly qualitative combined with a quantitative method. An extensive literature review was conducted in the area of access control and EHRs while the selected literature was analysed quantitatively using content analysis. Lastly, the expert review method was used to evaluate the proposed model which resulted in feedback that was analysed qualitatively using narration. The data collection and analysis methods, which were used on the secondary data, are discussed next.

2.5.1. Secondary Data

Secondary data is defined as data that is publicly available to the researcher and is relevant to the topic being studied (Wahyuni, 2012). The secondary data that was collected consisted of the literature which was categorised into themes in the area of access control and EHRs. This secondary data consisted of conference proceedings, journal articles, books and other online articles.

Additionally, secondary data was also collected to be used as a sample for the content analysis method. The content analysis sample was obtained by conducting a systematic literature review based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-

Analyses) flow diagram (Moher, Liberati, Tetzlaff, Altman, & The PRISMA Group, 2009). The initial secondary data went through four phases: identification, screening, eligibility and included as illustrated in Figure 7.1. The systematic literature review is discussed in more detail in Chapter 7: Section 7.2.1. At the end of the systematic literature review, the returned sample comprised of 24 journal papers. The sample was then imported into the MAXQDA software programme which was used for performing the content analysis of the sample. The sample which was used for the content analysis is available in Appendix B.

Regarding the literature review, an extensive literature review was conducted in the focused area using critical thought. This was done under the following four chapters: national EHR adoption internationally, regulations for a compliant national EHR system, securing the EHR through access control and standards for an interoperable national EHR system. Each of these chapters correspond to a sub-question which was derived from the main research question (as discussed in Chapter 1: Section 1.3). The results of conducting the literature review informed the proposed model which was used to address the research problem. The content analysis method is covered in more detail below.

2.5.1.1. Content Analysis

Content analysis is a method for making replicable and valid inferences from texts (Krippendorff, 2013). The use of this method leads to replicable results since researchers who use this method should be able to arrive at the same result when studying the same phenomena. Thus, the reliability of results is also ensured. Validity is also important when using the content analysis method. Validity is ensured when the categories resulting from the coding process effectively represent the concepts from the research question (Schreier, 2012). Validity in this instance was ensured since the created categories represented parts of the research question including ‘access control’ and ‘electronic health record'. Content analysis consists of interpreting the meanings from textual data (Wahyuni, 2012). This process results in the transformation of qualitative data into numeric data. Certain parts of the qualitative data are labelled using codes after which the number of occurrences of these codes throughout the data is calculated. Wahyuni (2012) refers to this as coding i.e. labelling where the assignment of a code represents a specific classification.

Figure 2.8 represents the content analysis method for answering the research question. Here texts represent the initial data that is selected and it is the context which will determine what these texts comprise of. As discussed earlier on, these texts comprised of journal papers in the area of access control and the EHR. Regarding the research question, this would be answered by the content analysis results that consist of the inferences made from the texts (Krippendorff, 2013).

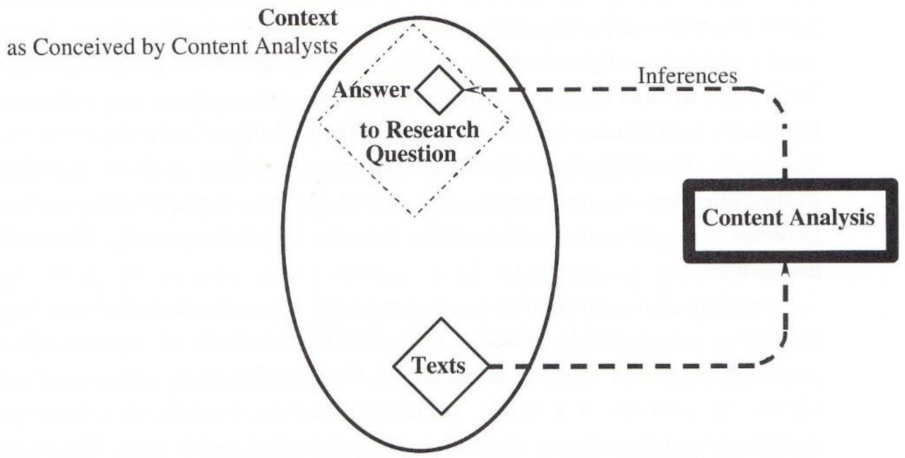


Figure 2.8: Answering the research question concerning a context of texts (Krippendorff, 2013)

The content analysis box in Figure 2.8 can be broken down into a number of components or steps: unitising, sampling, recording/coding, reducing, inferring and narrating (Krippendorff, 2013). Unitising consists of differentiating texts by providing definitions for relevant units. Next, sampling comprises of generating a content analysis sample that is representative of the population. Thirdly, coding involves the transformation of texts into analysable representations which result in tagged codes. The codes from the previous step can result in large amounts of data. Thus, the reducing step is important as it is used to reduce the coding

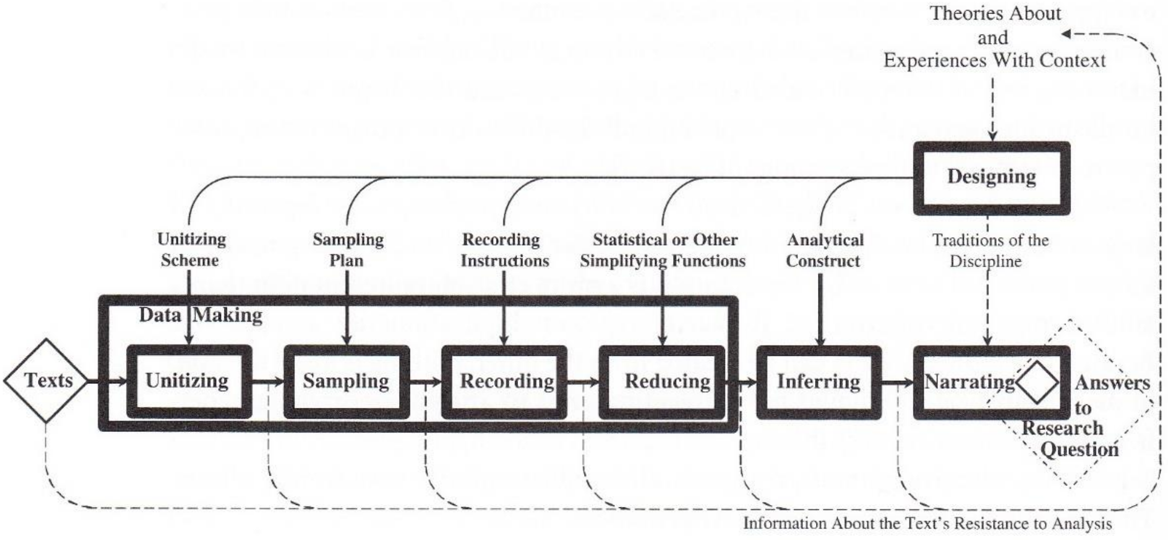


Figure 2.9: Components of content analysis (Krippendorff, 2013)

data to a manageable amount. Next, inferring involves relying on established analytical constructs in order to interpret the meaning of the texts. In the final component, narrating, the researcher makes the results of the content analysis method understandable to others. This would also include how the content analysis results answer the research question.

Figure 2.9 illustrates the six components of content analysis that were discussed above. The first four components together are known as ‘data making’ which consists of the creation of data from raw texts. Iteration is included in the content analysis method. Thus, the six components do not need to be followed in a linear manner. For instance, the reducing step may be executed repeatedly until the codes are reduced to a manageable amount. Lastly, the dashed lines in Figure 2.9 indicate another path which may be taken in the event that the analytical steps are not appropriate (Krippendorff, 2013). The data collection and analysis methods used under primary data are discussed next.

2.5.2. Primary Data

Primary data consists of new data that has not been collected before (Saunders et al., 2009). This new data was generated from the content analysis process, which initially resulted in 228 unique codes (the top 30 codes before reduction are available in Chapter 7: Table 7.1). In the end, these codes were reduced to 12 codes i.e. categories (the content analysis results are discussed in Chapter 7: Section 7.2.2). The 12 codes were used to inform the proposed model.

Primary data was also collected from the evaluation of the proposed model via an expert review. An expert review is a method for obtaining feedback from experts (Angkananon, Wald, & Gilbert, 2013). The expert review was conducted to evaluate the credibility of the proposed model. The expert review consisted of 10 experts. The chosen experts consisted of 5 security experts and 5 health experts (the health experts comprised of health IT experts and medical doctors). Despite the smaller population, the expert review was selected for evaluating the proposed model since it meets design science research guideline 3 (which was discussed in Section 2.3.4.2). A presentation was sent to the chosen experts containing the proposed model along with both closed-ended and open-ended questions (the expert review questions are available in Appendix A). The expert reviewers were invited to respond using Google Forms. This resulted in primary data being collected in the form of feedback from the results of the expert review.

The received feedback was analysed using narration. This was used to further refine the proposed model. The expert review results are available in Chapter 7: Section 7.3. In the next section, ethical considerations pertaining to this study are covered.

2.6. Ethical Considerations

Ethics as it relates to research (i.e. research ethics) is defined as the appropriateness of the researcher's behaviour relative to those who become the subject of the research and are consequently affected by it (Saunders et al., 2009). Research ethics relates to questions on how the research topic is created and explained, how the research is designed, how access to data is gained, collected, stored and analysed and how the research findings are written up in a moral way. This study required input from experts, in the form of feedback, via an expert review. This study abided by a number of principles for ethical conduct in research including honesty, openness, respect for intellectual property and confidentiality (Shamoo & Resnik, 2015). These principles are highlighted below:

- **Honesty**: The communications of the study were honestly reported. This included the honest reporting of the methods used, results and publications.
- **Openness**: The principle of openness was also followed when receiving feedback from the expert review.
- **Respect for intellectual property**: Respect for intellectual property was ensured by acknowledging the research contributions made by others.
- **Confidentiality**: The confidentiality of the expert reviewers, who participated in the study, was preserved by ensuring that they remained anonymous.

Ethical clearance was obtained from the Rhodes University Ethics Committee (ethical approval number: CIS18-03) before the selected expert reviewers participated in the study. The chapter concludes in the next section.

2.7. Summary

In this chapter, the research design and methodology which were used in this study were discussed. The research design and methodology structure was firstly examined in terms of the layers of the research onion. This was followed by the comparison of four research paradigms: positivism, interpretivism, pragmatism and design science. Design science was selected as the most suitable research paradigm for this study due to the creation and evaluation of an artefact which is appropriate for addressing the research problem. The design science paradigm was further discussed in terms of the IS research framework and the design science research guidelines. The research methods were subsequently covered which included quantitative, qualitative and mixed methods with mixed methods being selected for this study. Next, the data collection and analysis methods were discussed which consists of the two main methods used: content analysis and the expert review. Finally, the ethical considerations in relation to this study were covered which included the principles of ethical conduct which were followed by this study. The next chapter covers the national EHR adoption internationally.

CHAPTER 3: NATIONAL ELECTRONIC HEALTH RECORD ADOPTION INTERNATIONALLY

3.1. Introduction

In this chapter, a number of countries are examined in terms of their adoption of the national EHR. These countries include Canada, New Zealand, South Africa, Sweden and England. The chapter begins by discussing the three types of health records including how one health record may comprise of another. Next, the current state of countries' national EHR systems are examined, focussing on each country's current situation with regards to the adoption of the national EHR. This is followed by the discussion of system architectures including the use of national EHR system architectures by the examined countries. Lastly, the challenges experienced by the countries' national EHR implementations, which serve as lessons learned, are covered for all five countries. This chapter assists with addressing the research problem since it provides insight on a national EHR system architecture that needs to be implemented before access control can be used to secure the national EHR system. The next section differentiates between the three types of health records.

3.2. Types of Health Records

Various types of health records have been used by the countries that will be examined in this chapter. It is important to differentiate between the different health records in order to understand the national EHR. A health record can be categorised into three main categories: Electronic Medical Record (EMR), EHR and Personal Health Record (PHR). These three health records are illustrated in Figure 3.1 along with the relationship between each type of health record. An EMR is an electronic record of an episode of medical care within a single health facility such as a hospital (CSIR & Department of Health, 2014). It is a partial health record since it contains part of a patient's information recorded at a certain health facility. Thus, the health facility controls the EMR. On the other hand, an EHR is a longitudinal electronic record of a patient's information which consists of one or more encounters in any health facility (Deloitte, 2015). Referring to Figure 3.1, Patient A's EHR comprises of health information which is received from the EMR systems located at Hospital A, B and C. Each of these three hospitals represent a patient encounter and could be located in a different region. In a national context, this EHR would also be known as a national EHR. Thirdly, the PHR is an electronic record which contains information about a patient over their lifetime and is

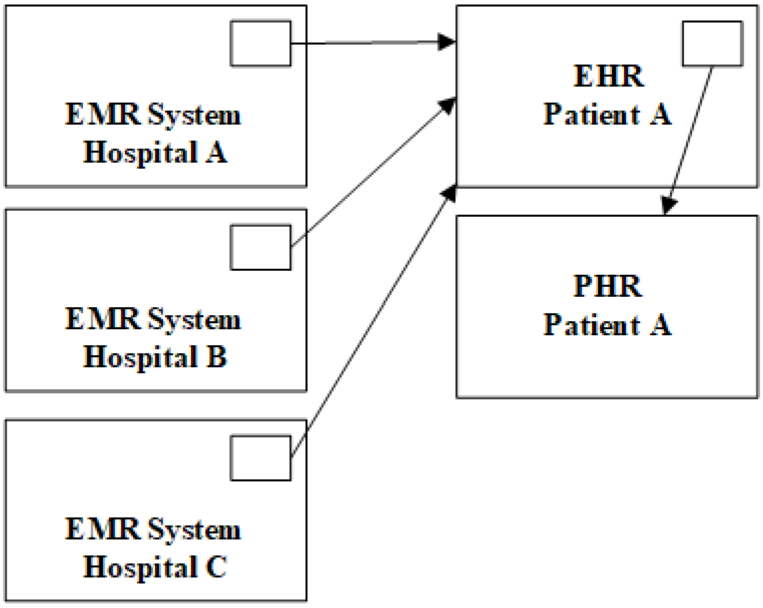


Figure 3.1: Visual representation of the different types of health records – adapted from Conover (n.d.)

managed by the patient (CSIR & Department of Health, 2014). As depicted in Figure 3.1, the PHR is a superset of the EHR as the PHR is made up of the EHR and information provided by the patient. The current state of the examined countries' national EHR systems is covered next.

3.3. Current State of Countries' National Electronic Health Record Systems

This section discusses the current state of national EHR systems with regards to the five countries that will be examined in this chapter: Canada, New Zealand, South Africa, Sweden and England. Most of the available literature focussed on Spine, England's national EHR system, as opposed to the other UK countries. As a result, England was included as part of the examined countries. Each of the examined five countries is at a different stage with regards to the national EHR system, with some countries having already implemented a national EHR system while other countries are still in the process of implementing a national EHR system. Additionally, each of these countries has experienced issues during the process of moving towards a national EHR system. The next section begins with a discussion of Canada's current state with regards to its national EHR system.

3.3.1. Canada

The health sector in Canada has been one of the first industries to adopt and use information systems for operational needs. These information systems have formed the foundation of EMR systems and have included the implementation of clinical, radiology, laboratory and drug information systems (Canada Health Infoway, 2006c). Despite this foundation, a lack of interoperability between systems and numerous health facilities lacking EMR systems has caused regional disparities (Chang & Gupta, 2015). As a result, this has had an impact on the progress of the national EHR. Up until 2015, EMR adoption in Canada was placed at 73% (Strasbourg, 2016).

3.3.2. New Zealand

Similar to Canada, New Zealand is also in a good position with regards to its health information systems which were adopted many years ago, forming the basis for New Zealand's EMR systems (Reid & Osborne, 2016). On the other hand, many hospitals possess different health information systems resulting in a lack of interoperability (Deloitte, 2015). The review of New Zealand's EHRs strategy by Deloitte (2015) also states that a move from a virtual EHR to a single national EHR is desired. The review defines a virtual EHR as systems which assemble disparate data on demand and display this combined data via interfaces and software. Although a single national EHR is not completely realised yet, a number of New Zealand general practices have provided their patients with internet access to their GP's medical records. According to the Ministry of Health (as cited in Wells, 2017), up until 2017, 47% of New Zealand general practices have implemented a portal with 407 049 patients having registered, representing approximately 10% of the New Zealand population.

3.3.3. South Africa

There is still a large amount of progress which needs to be made before South Africa achieves a national EHR. A majority of health facilities in South Africa are currently using paper-based systems (CSIR & Department of Health, 2014). On the other hand, some South African hospitals have implemented EMR systems. For instance EMR systems, including pharmacy

Table 3.1: Patient management/hospital information systems currently deployed in public sector facilities in South Africa (Department of Health South Africa, 2012)

Province	Patient Management/Hospital Information Systems in use
Eastern Cape	Delta 9
Free State	Meditech; PADS
Gauteng	Medicom; Soarian MedSuite; PharmAssist; PAAB
KwaZulu-Natal	Medicom; Meditech; PALS; Pro-Clin; ReMed
Limpopo	Medicom
Mpumalanga	PAAB
North West	PAAB
Northern Cape	Nootroclin
Western Cape	Clinicom; Delta 9; PHCIS; JAC Pharmacy

and radiology systems, have been implemented in the Western Cape (Department of Health South Africa, 2012). However, due to a variety of proprietary systems (as depicted in Table 3.1) being used in South Africa's nine provinces, they have not been able to exchange information due to a lack of interoperability. Figure 3.2 illustrates the total number of health information systems deployed in each province. The Western Cape has deployed the most number of health information systems, while Limpopo has deployed the least number of systems (CSIR & Department of Health, 2014).

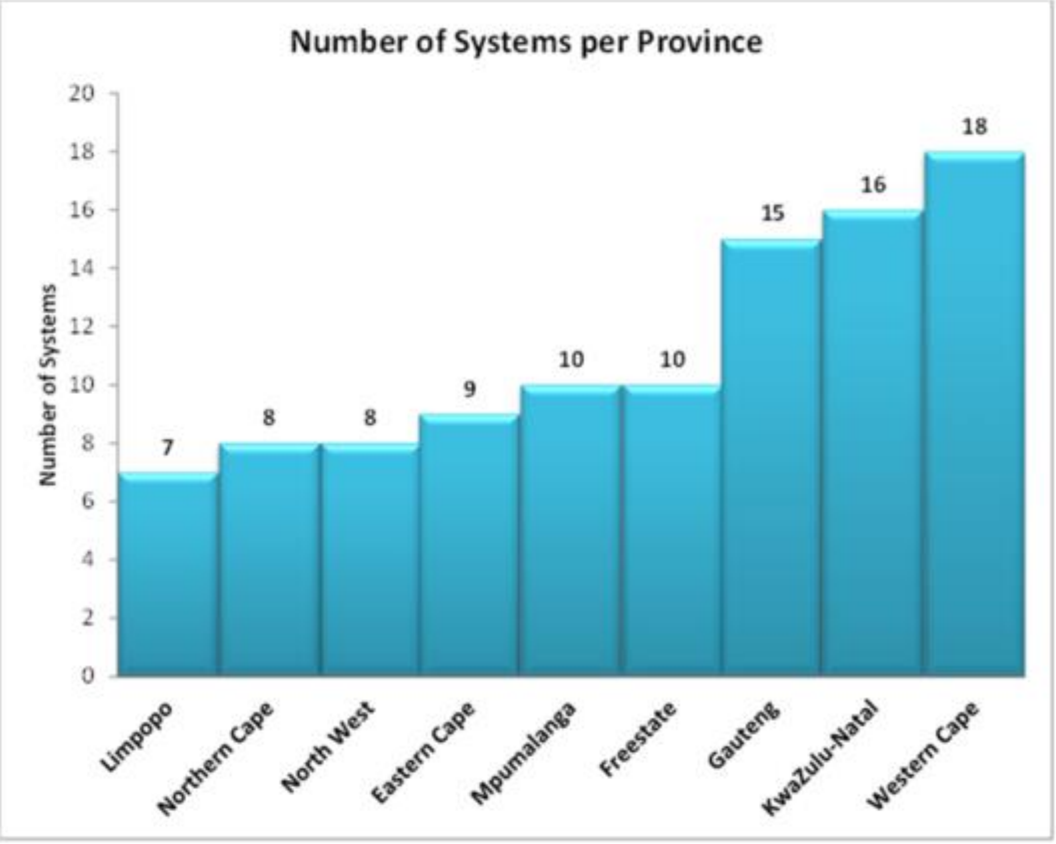


Figure 3.2: Total number of health information systems deployed per province (CSIR & Department of Health, 2014)

3.3.4. Sweden

Sweden is at an advanced stage of providing access to a national EHR. Disparate EMR systems have been able to exchange information through the use of a national HIE platform (Hägglund & Scandurra, 2017). By accessing a patient portal via 1177.se, patients are able to access their EHR through the use of a national e-service called Journalen. As cited by Hägglund and Scandurra (2017), up until December 2016, 17 out of the 21 Swedish counties have provided access to EHR information via Journalen. Additionally, in 2016, 34.1% of the Swedish population had created an account for the 1177.se portal to use e-services including Journalen. While Journalen is used by patients to access their EHR, the National Patient Summary e-service is used by clinicians to access their patients' EHRs, as long as the patient has provided their consent (Ministry of Health and Social Affairs, 2010).

3.3.5. England

England's aim to realise a national EHR has experienced a number of challenges. Launched in 2002, the National Health Service (NHS) National Programme for Information Technology (NPfIT) was an initiative to move England to a national and integrated EHR (Takian & Cornford, 2012). The aim was for medical records to be created locally, while also being sharable across different health facilities. Also specified as part of the NPfIT was Spine, a central system used in combination with local systems to deliver the EHR known as the SCR (House of Commons, 2007). Despite all of this, the NPfIT encountered many issues. Some of these issues are discussed in Section 3.5. As a result, the NPfIT was brought to an end in 2011 (Takian & Cornford, 2012). Consequently, a new approach was created which included retaining Spine (Reid & Osborne, 2016). Currently, patients are able to access their GP SCR. According to NHS England (as cited in Parliamentary Office of Science and Technology, 2016), in April 2014, the percentage of GP surgeries in England which allowed patients to access their SCR online increased from 3% to 97%. Additionally, 0.4% of patients have accessed their SCR online. In the next section, the different types of system architectures used by the examined countries are discussed.

3.4. Electronic Health Record System Architectures

The system architectures discussed in this section have either been implemented by the examined countries or are still at the conceptual stage. The system architectures include the centralised and distributed architectures and will be discussed in terms of how they will be used to realise a national EHR. The summary of these two system architectures is depicted in Table 3.2 as a comparison using their characteristics. The centralised architecture is covered first.

3.4.1. Centralised Architecture

In a centralised architecture, copies of patient information are transferred periodically from local health facilities to a central system which functions as a repository (AlJarullah & El-Masri, 2013). When a request is made to retrieve a patient's complete EHR, this is retrieved from the central repository. The centralised architecture is depicted in Figure 3.3.

AlJarullah and El-Masri (2013) mention a number of advantages of the centralised architecture. The speed of running a query for a patient's EHR is faster than the distributed architecture since all of the information is retrieved from one central repository. Secondly, the centralised architecture is easier to maintain than the distributed architecture since all patient information

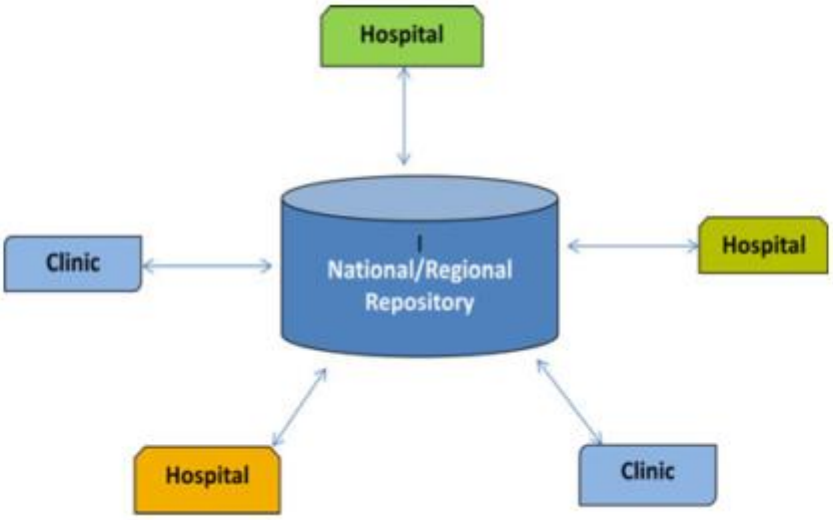


Figure 3.3: Centralised architecture (AlJarullah & El-Masri, 2013)

is located centrally. Another advantage with the centralised architecture is that there is centralised control over all patient information which is stored in the centralised repository (Jalal-Karim & Balachandran, 2008).

On the other hand, there are a number of disadvantages with the centralised architecture which are mentioned by AlJarullah and El-Masri (2013). Since copies of patient information are transferred at set times from health facilities to a central system, patient information stored in the central system may not always be up-to-date. There is also a security risk with storing all of the patients' information in one central location. The use of a central system is also a single point of failure: if the central system goes down, patients' national EHRs will be unavailable. Lastly, there is a duplication of information since the central system stores duplicate patient information (Jalal-Karim & Balachandran, 2008). The distributed architecture, which addresses some of these disadvantages, is discussed next.

3.4.2. Distributed Architecture

In a distributed architecture, patient information is stored and managed locally at each health facility (AlJarullah & El-Masri, 2013). Centrally maintained links are stored in a central system and contain the original location of the patient's information i.e. the location of the health facility where the patient's information is stored. When a request is made for a patient's EHR, the central system will query the various health facilities where parts of the patient's information reside. The central system will then return the aggregated EHR representing all of the patient's encounters. The distributed architecture is illustrated in Figure 3.4.

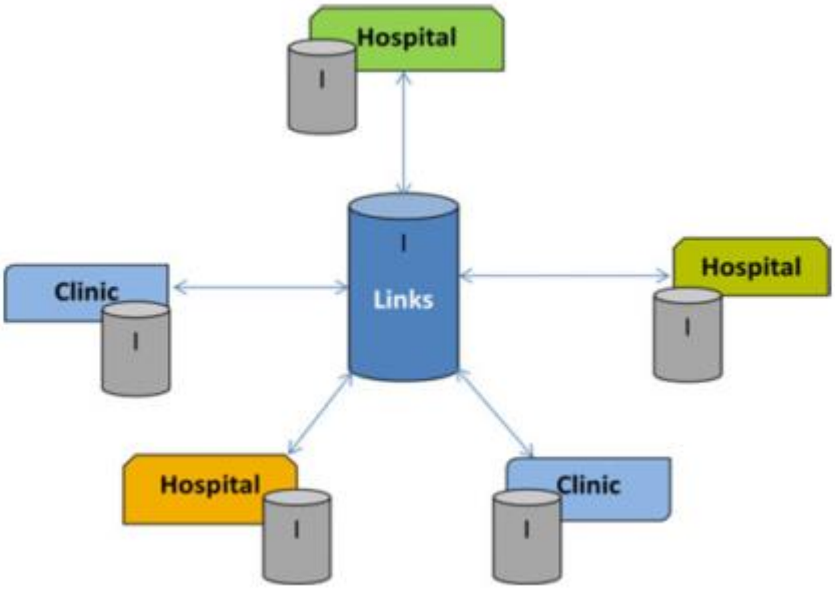


Figure 3.4: Distributed architecture (AlJarullah & El-Masri, 2013)

The distributed architecture has a number of advantages as mentioned by AlJarullah and El-Masri (2013). Firstly, the latest patient information is accessed from the source health facility where it is located. Additionally, there is no duplication of patient information as only one instance is located at the source health facility. Thirdly, there is an increased level of security in the distributed architecture as opposed to the central architecture. This is because patient information remains at the source health facility instead of being duplicated in a central system. Since patient information is located at different health facilities, there is no single point of failure. Jalal-Karim and Balachandran (2008) mention another advantage of autonomy where local health facilities have control over patient information stored at the health facility.

Despite the advantages mentioned, there are also disadvantages with the distributed architecture. A high amount of network traffic can arise when accessing patient information stored across a large number of health facilities, potentially resulting in delays. The distributed

Table 3.2: Comparison of system architectures by characteristic – adapted from (Jalal-Karim & Balachandran, 2008; AlJarullah & El-Masri, 2013)

Characteristic	Centralised Architecture	Distributed Architecture
Speed	Fast speed of running query for patient’s information	Possible delays due to increased network traffic
Control	Centralised control over all patient information	Health facilities have autonomy over local patient information
Consistency	Centralised patient information not always up-to-date	Latest patient information available from health facility
Security	Security risk with centrally stored patient information	Increased level of security
Reliability	Single point of failure	No single point of failure
Redundancy	Duplication of patient information	No duplication of patient information
Maintainability	Easier to maintain	Harder to maintain

architecture is also harder to maintain than the centralised architecture since parts of a patient's information are distributed across a large number of health facilities (AlJarullah & El-Masri, 2013). The examined countries' national EHR system architectures are covered next.

3.4.3. Architectures of Five National Electronic Health Record Systems

The system architectures of the five examined countries: Canada, New Zealand, South Africa, Sweden and England are discussed below in terms of their relevant components that function together to operate a national EHR system. Also included in the discussion is the type of system architecture used: the centralised architecture or distributed architecture. Table 3.3 indicates the type of system architecture (potentially) used by each country. The next section begins with a discussion of Canada's EHR solution.

Table 3.3: Type of system architecture (potentially) used by examined countries

Country	Centralised Architecture	Distributed Architecture
Canada	✓	
New Zealand	✓	
South Africa	✓	
Sweden		✓
England	✓	

Compiled from: (AlJarullah & El-Masri, 2013; Canada Health Infoway, 2006b; CSIR & Department of Health, 2014; Deloitte, 2015; Sellberg & Eltes, 2017)

3.4.3.1. *Canada*

Canada's EHR solution blueprint includes the EHR solution (Figure 3.5) which contains the EHR Infostructure (EHRi) (Canada Health Infoway, 2006b). The EHRi is a group of components that support health information management applications. The applications include point of service applications and EHR viewers for viewing patient information. Patient information recorded on a point of service application is replicated into the EHR via the EHRi. Thus, the EHR solution uses a centralised architecture. The EHR solution blueprint discusses the various components of the EHRi (Canada Health Infoway, 2006b). Registries data and services comprise of registries which store, maintain and provide information which is required to uniquely identify entities in the EHR e.g. client registry, provider registry and location registry. The EHR data and services component comprises of domain repositories that maintain and store specific clinical information such as the shared health record and laboratory repositories. Next, both the health information data warehouse and ancillary data and services components use EHR information for additional purposes such as research. The longitudinal record services component collects patient information from the local EHRi and is also able to retrieve and merge patient information from other infostructures located in different regions,

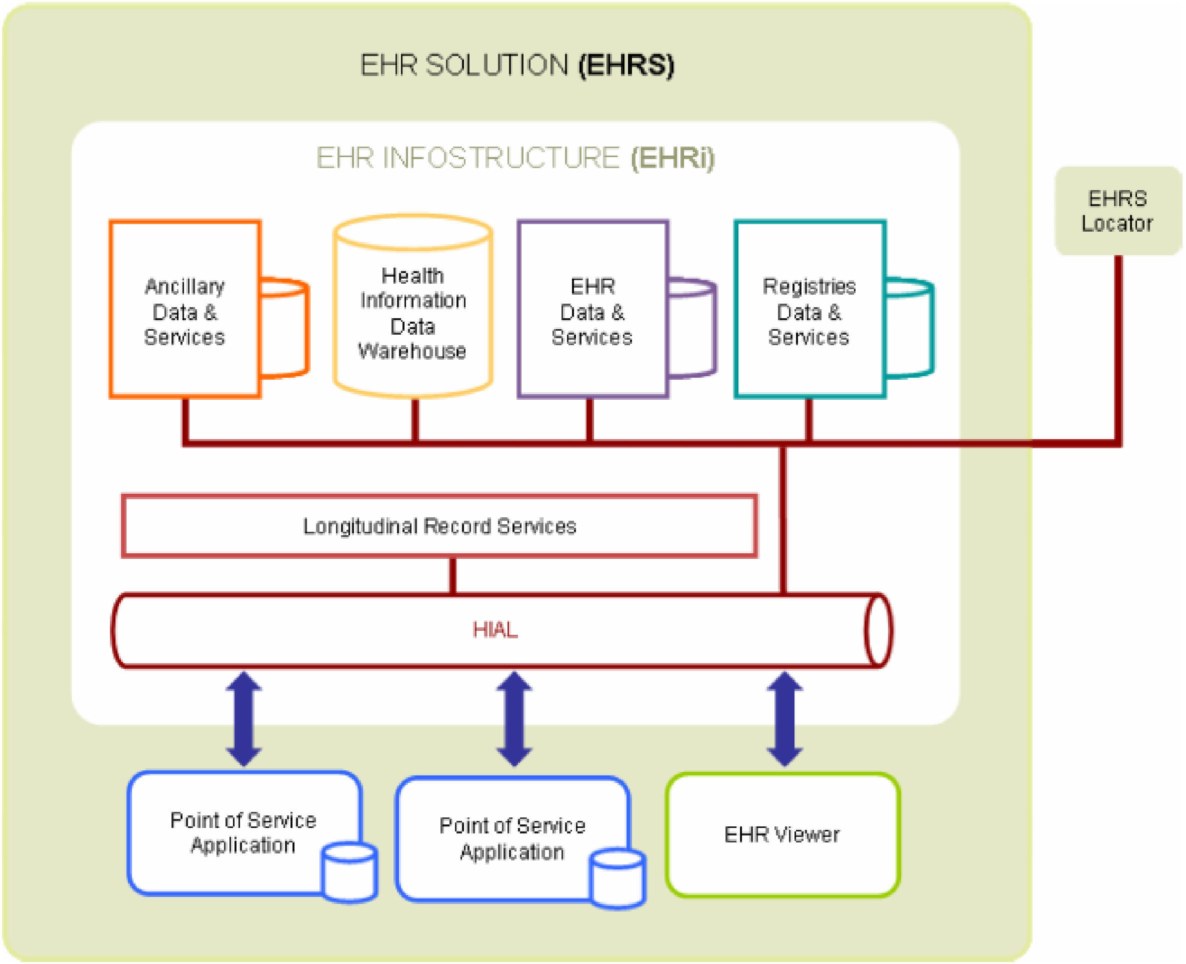

EHR SOLUTION (EHRS)
EHR INFOSTRUCTURE (EHRi)
EHRS Locator
Ancillary Data & Services
Health Information Data Warehouse
EHR Data & Services
Registries Data & Services
Longitudinal Record Services
HIAL
Point of Service Application
Point of Service Application
EHR Viewer

Figure 3.5: EHR Solution (Canada Health Infoway, 2006b)

thus forming a longitudinal record. Next, the Health Information Access Layer (HIAL) is an interface which acts as a gateway between point of service applications and the EHRi. The HIAL consists of services such as privacy and security services (access control, secure auditing, etc.) and interoperability services which are applied to every request made by a point of service application. Lastly, the EHR solution locator contains addresses pointing to other infostructures where specific patient information is located and these locations are queried by the longitudinal record services. Next, New Zealand's conceptual national EHR system is examined.

3.4.3.2. *New Zealand*

The review of New Zealand's EHRs strategy by Deloitte (2015) states that New Zealand's regional systems have been linked to national systems using a point-to-point model. Within this point-to-point model, the virtual EHR approach has been used where fragmented information is assembled on demand and viewed on screen. New Zealand has chosen to move away from the virtual EHR to a single EHR i.e. national EHR. Moving towards a national EHR involves foregoing the point-to-point model for the hub and spoke model. In the hub and spoke model, local systems all connect into one central system. Deloitte (2015) illustrates a visual representation of a potential national EHR (Figure 3.6) which is in the form of a hub and spoke model. Here a number of EMR systems, located at different health facilities, contain patient information that is fed into a central repository. Thus, a centralised architecture is used where the EHR is represented in the centre as a longitudinal record representing the patient's complete journey. Two other important components which will also be vital for the functioning of the national EHR are New Zealand's national registries: the national health index and health provider index. The national health index is used for uniquely identifying patients, while the health provider index is used for uniquely identifying health providers. A potential system architecture for South Africa's national EHR is covered next.

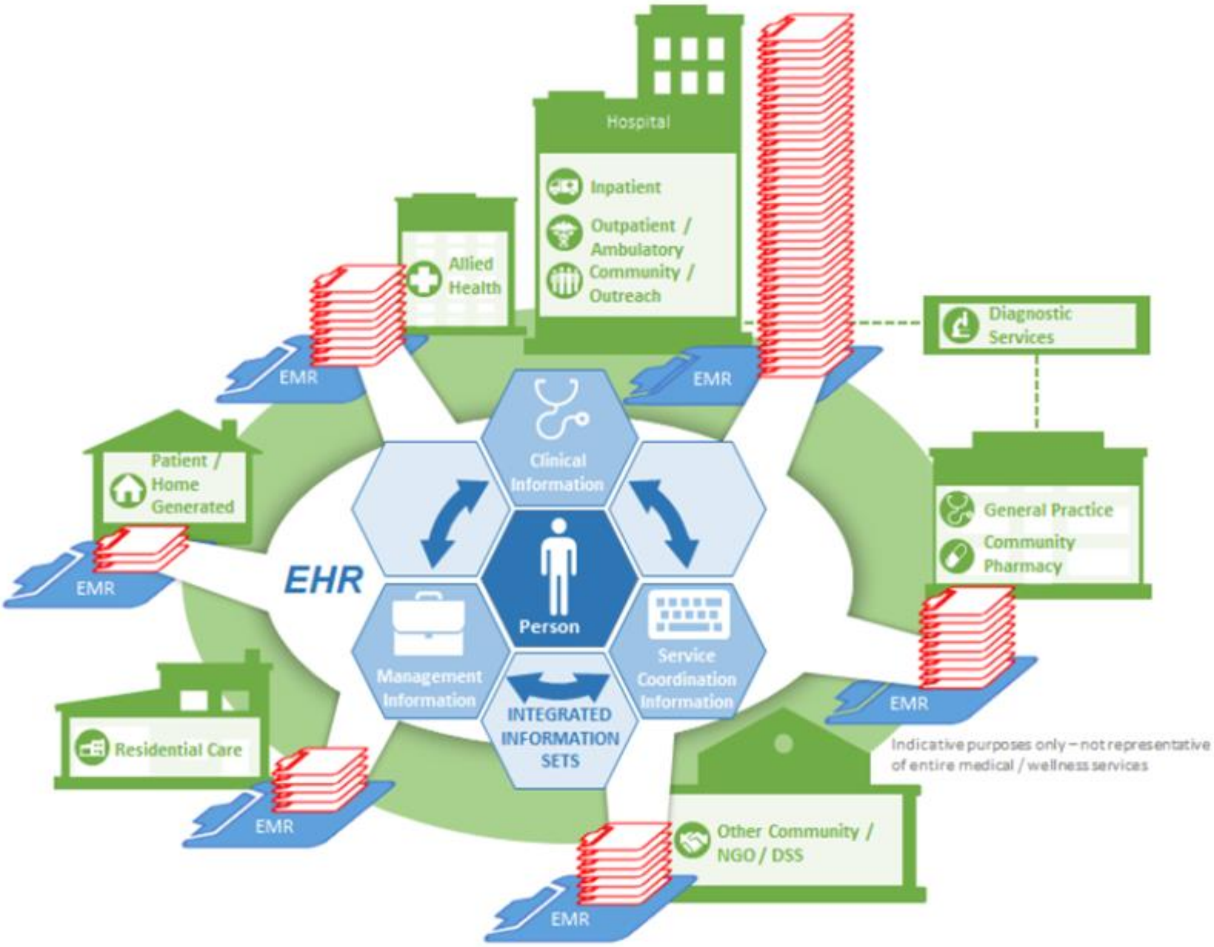


Figure 3.6: National Electronic Health Record (Deloitte, 2015)

3.4.3.3. *South Africa*

CSIR and Department of Health (2014) discuss a potential fully integrated national shared EHR system (Figure 3.7) for the South African context. This EHR system consists of various components. Demographic registries comprise of the storage and maintenance of demographic information relating to entities such as patients, healthcare providers and health facilities. For instance, the patient registry, i.e. Patient Master Index (PMI), is shared with all health facilities allowing the patient to have the same identifier across all health facilities. The patient registry also enables searching for patients using parameters such as the patient's name. Similarly, the provider registry and facilities registry can be queried in order to retrieve healthcare providers and health facilities respectively. The clinical repositories component involves the storage of information relating to healthcare events. Patient information is stored in local EMR systems, while part or all of this information is also stored centrally in the shared EHR. Hence, a centralised architecture is used. Clinical repositories including the shared EHR are shared

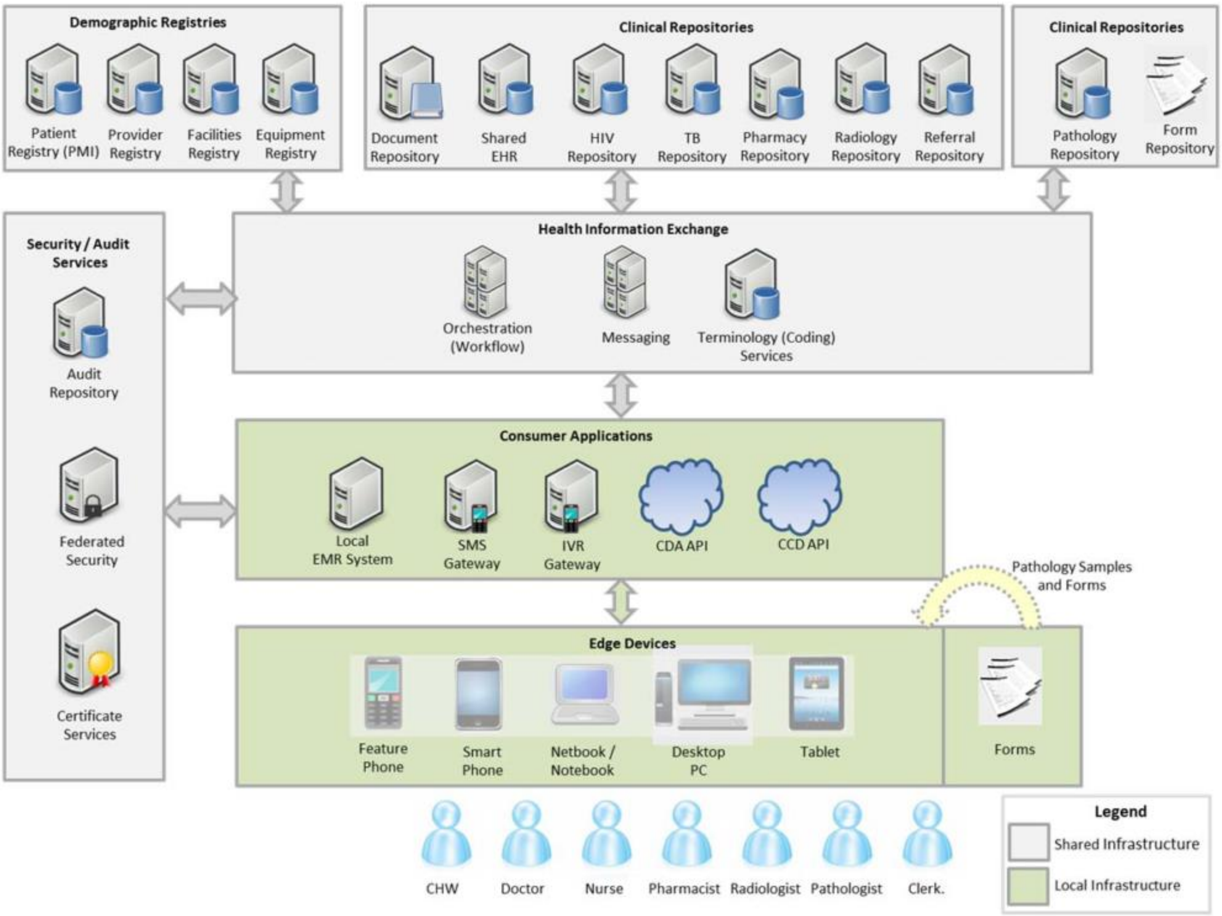


Figure 3.7: Fully integrated national shared electronic health record system (CSIR & Department of Health, 2014)

nationally and can be updated by authorised users at all health facilities connected to the shared infrastructure. The next component, HIE, is the middleware used for the integration of regional registries and clinical repositories. It also provides a single set of interfaces through which consumer applications can communicate with registries. Another important component is security/audit services, a set of federated services which are used by HIE, registries, repositories and clients to facilitate authentication and auditing. Consumer applications, located at the local health facility, are used to integrate edge devices into the system and also manage messages which are required for viewing and recording information in the shared infrastructure. Lastly, the edge devices component consists of hardware devices used by clinicians to access consumer applications including accessing patient information. CSIR and Department of Health (2014) recommend that a cloud-based shared national infrastructure, similar to the fully integrated infrastructure in Figure 3.7, be used. The proposed model, which introduces an alternative EHR system architecture for South Africa's national EHR system, is covered in Chapter 8: Section 8.6. While the security of the national EHR system in Figure 3.7 is represented by the security/audit services component, the proposed model includes an access control component for securing the EHR. The theoretical foundation of this study (ANSI RBAC standards and Clark-Wilson model) determines how access control is enforced in the proposed model. The Swedish eHealth architecture, including the national EHR, is discussed next.

3.4.3.4. *Sweden*

The Swedish eHealth architecture, represented in Figure 3.8, consists of the national HIE platform, which is the main component that enables the realisation of a national EHR and is covered in this section. The national HIE platform represents all participating regional health information systems as a single virtual national EHR system (Sellberg & Eltes, 2017). Patients can use Journalen to access their virtual national EHR (Hägglund & Scandurra, 2017). On the other hand, clinicians can access their patient's national EHR using the National Patient Summary as long as the patient has provided their consent (Ministry of Health and Social Affairs, 2010). Journalen and the National Patient Summary are both e-services and thus fall under the service consumers component. Sellberg and Eltes (2017) also mention that all requests are processed by the source system, where the requested patient information is located, in real time. Thus, Sweden uses a distributed architecture and is unique in comparison to the other examined countries which all use the centralised architecture. The national HIE platform

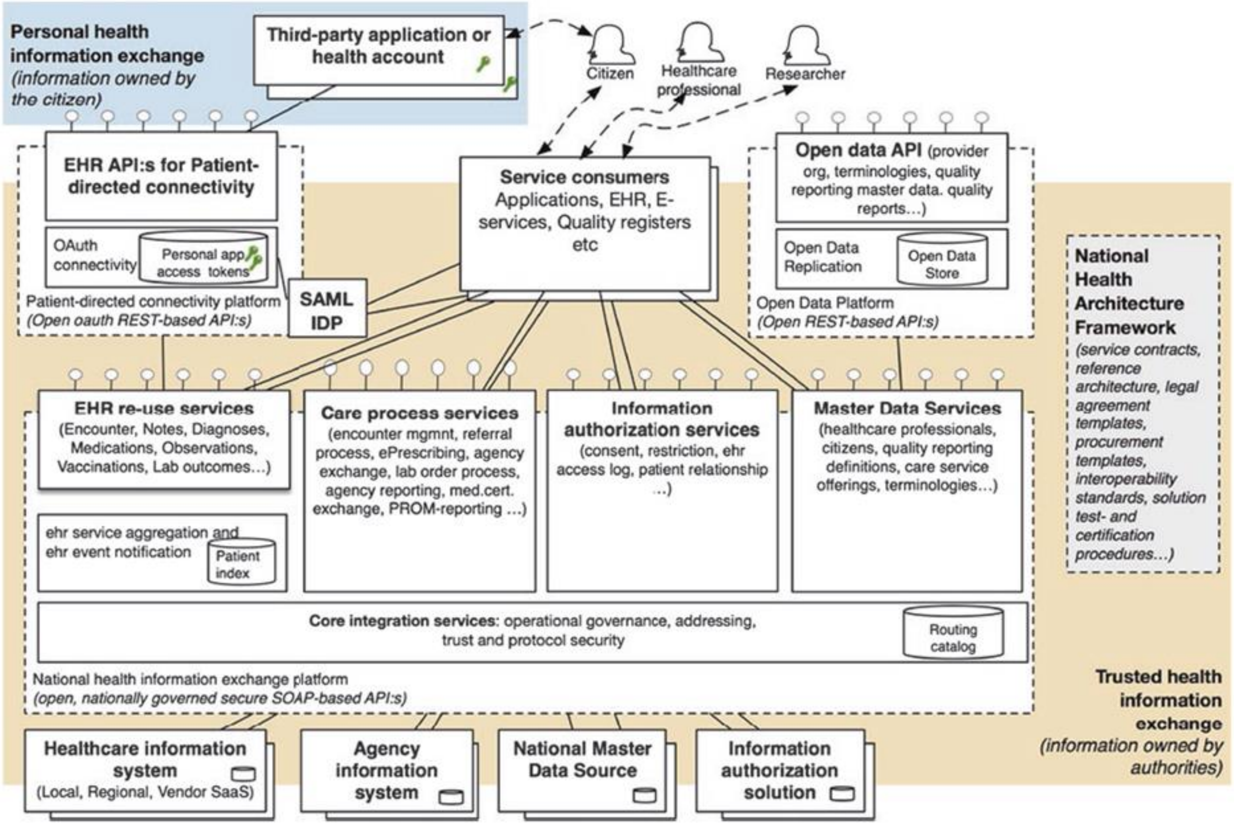

Personal health information exchange (information owned by the citizen)
Third-party application or health account
Citizen
Healthcare professional
Researcher
EHR API:s for Patient-directed connectivity
OAuth connectivity
Personal app access tokens
Patient-directed connectivity platform (Open oauth REST-based API:s)
SAML IDP
Service consumers Applications, EHR, E-services, Quality registers etc
Open data API (provider org, terminologies, quality reporting master data. quality reports…)
Open Data Replication
Open Data Store
Open Data Platform (Open REST-based API:s)
National Health Architecture Framework (service contracts, reference architecture, legal agreement templates, procurement templates, interoperability standards, solution test- and certification procedures…)
EHR re-use services (Encounter, Notes, Diagnoses, Medications, Observations, Vaccinations, Lab outcomes…)
Care process services (encounter mgmnt, referral process, ePrescribing, agency exchange, lab order process, agency reporting, med.cert. exchange, PROM-reporting …)
Information authorization services (consent, restriction, ehr access log, patient relationship …)
Master Data Services (healthcare professionals, citizens, quality reporting definitions, care service offerings, terminologies…)
ehr service aggregation and ehr event notification
Patient index
Core integration services: operational governance, addressing, trust and protocol security
Routing catalog
National health information exchange platform (open, nationally governed secure SOAP-based API:s)
Trusted health information exchange (information owned by authorities)
Healthcare information system (Local, Regional, Vendor SaaS)
Agency information system
National Master Data Source
Information authorization solution

Figure 3.8: Swedish eHealth architecture (Sellberg & Eltes, 2017)

depends on a number of utility services such as the patient index, which supports the aggregation of information. The national HIE platform is also used for trusted HIE and personal HIE. Trusted HIE is the exchange of information owned by Swedish county councils, while personal HIE is the exchange of information owned by patients. Personal health information is obtained from source systems via the national HIE platform. Once under the ownership of the patient, this information can be shared with third party apps such as eHealth apps. Next, England's national EHR system is examined.

3.4.3.5. *England*

England's national EHR system is based on the NHS Care Records Service, which was part of the NPfIT (House of Commons, 2007). The NHS Care Records Service (Figure 3.9) comprises of a central system known as Spine and local systems, which are delivered by local service providers. Although the NPfIT does not exist anymore, parts of it have been retained in the current national EHR system such as Spine (Reid & Osborne, 2016). Additionally, in 2014, Spine was migrated to an open source system having previously run on a proprietary system (Clarke, 2014). Spine consists of various components. The Personal Demographics Service stores demographic information of patients including the NHS number, which acts as the unique patient identifier (AlJarullah & El-Masri, 2013). Next, SCRs, which are created on

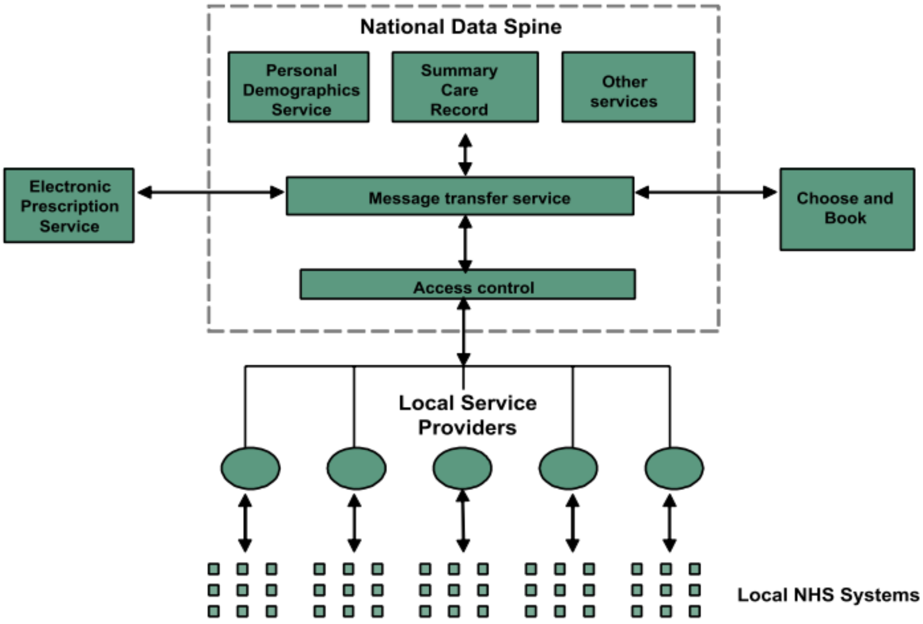


Figure 3.9: NHS Care Records Service (House of Commons, 2007)

local systems by clinicians, are also stored on Spine. Hence, a centralised architecture is used. Patients are able to access their SCR through the internet by using a portal. The message transfer service is used to route clinicians' message requests from the local systems to the services which they request such as the SCR and Electronic Prescription Service (House of Commons, 2007). Access control is also used to control access to various services. In the next section, the challenges experienced by the examined countries' national EHR implementations are discussed.

3.5. Challenges Experienced by Countries' National Electronic Health Record Implementations

In this section, the challenges faced by the examined countries, during their national EHR implementations, are discussed. These challenges can be used as lessons learned for future national EHR implementations. The examined countries, which are currently not at the national EHR stage, are discussed with regards to the challenges experienced while utilising EMR systems which form the foundation for the national EHR. The challenges faced by the examined countries are summarised in Table 3.4. The first challenge, concurrent use of paper and EHRs, is discussed next.

3.5.1. Concurrent Use of Paper and Electronic Health Records

The countries' aim of achieving a national EHR system has been negatively impacted by the concurrent use of paper and EHRs. This challenge comprises of the simultaneous use of both paper-based records and EHRs (or EMRs where the country has not yet reached the national

EHR stage) by clinicians. This challenge in the Canadian context is discussed in more detail below.

Canada

Physicians in Canada have been using paper-based records and EMR systems concurrently. According to the National Physician Survey (as cited in Chang & Gupta, 2015) which was conducted in 2010, numerous Canadian physicians mentioned that they either used standalone EMR systems or that they used EMR systems in combination with paper-based records. Using an EMR system in combination with paper-based records acts as a barrier to Canada's aim of moving towards an interoperable EHR since paper-based records cannot be shared as easily as the EHR. Additionally, interoperability cannot co-exist with paper-based records and would require that paper-based records are not concurrently used with EMR systems.

New Zealand

Some health facilities in New Zealand have also used a combination of paper-based records and EMR systems. Deloitte (2015) mention that clinicians may find that EMR systems do not provide all the required information, leading them to additionally use paper and pen. This creates two problems: the need to reference both paper and system files and the re-keying of information e.g. the re-keying of eReferrals into some district health board systems. This leads to the problem of duplication which results in a loss of productivity due to more time being spent on using both paper-based records and EMR systems. This is in contrast to increased productivity which the EMR system aims to provide. Thus, this benefit can only be attained if EMR systems are utilised without paper-based records.

South Africa

There are many hospitals in South Africa which utilise both paper-based records and EMR systems. Khayelitsha Hospital is one example where paper-based records and an EMR system, known as Clinicom, are both used simultaneously (Ohuabunwa et al., 2016). The motive for using paper-based records is that they can be shared within the hospital and neighbouring hospitals by scanning the paper-based records into an online database through enterprise content management. Although sharing patient information is important for the delivery of healthcare, sharing is limited to within the hospital and neighbouring hospitals and would not be sustainable in supporting the sharing of patient information nationally. Ohuabunwa et al. (2016) mention the disadvantages of using paper-based records which include difficulty reading handwriting (which can lead to medical errors) and missing notes. These disadvantages can be avoided by forgoing paper-based records for EMR systems. An additional example of the concurrent use of paper and an EMR system is mentioned by Weeks (2014) who states that a Pretoria clinic utilised paper-based records and an EMR system together. This clinic had adopted what was known as a 'paper-based culture'. Without proper change management in place to move towards the use of EMR systems, clinicians will still follow the paper-based culture.

Sweden

Although Sweden has a national HIE platform for accessing the national EHR, it has experienced problems at the regional level. Rexhepi, Ahlfeldt, and Persson (2015) mention a hospital in Västra Götaland, a Swedish county, which encountered issues with regards to the concurrent use of paper-based records and EMR systems. In addition to working with a patient's EMR, clinicians also manually handled the same information. This comprised of importing printed copies of the paper-based record into the receiving EMR system, which could not electronically receive the same information. This was done by scanning or manually entering the patient information from the paper-based record into the EMR system. This created problems of inefficiency and increased the risk of making errors. This was due to the fact that patient information, which was meant to be imported into the receiving EMR system, may have been missed leading to a 'gap' in the EMR. This gap in the EMR can only be filled if paper-based records are not manually entered into the system and that the same information is received electronically.

England

England has also experienced the concurrent use of paper-based records and EMR systems due to the limited functionality of EMR systems at its hospitals. One such event occurred in 2014 with the EMR system which was deployed at Cambridge University Hospitals (Parliamentary Office of Science and Technology, 2016). There were problems which the clinicians experienced with the EMR system's functionalities when it went live, while some functionalities were not included in the system. As a result, the clinicians went back to using paper-based records due to the fact that the EMR system had limited functionality. Hence, it is crucial that all necessary functionalities are included in the EMR system before it gets deployed. Lack of patient adoption of EHRs, which is the second challenge, is covered below.

3.5.2. Lack of Patient Adoption of Electronic Health Records

This section covers the lack of patient adoption of EHRs, which also includes PHR adoption issues in Canada. In contrast to the previous challenge (concurrent use of paper and EHRs) that focussed on the clinician, this challenge is experienced by the patient. Also discussed are a number of barriers that enable this challenge such as the lack of computer literacy and patient interest. Out of the five examined countries, both New Zealand and South Africa did not have the required information for this challenge. The lack of adoption of the PHR by patients in Canada is discussed next.

Canada

Regarding the adoption of the PHR by patients, the study of Gagnon et al. (2016) mention that the adoption of the PHR depends on the health literacy and computer literacy of the patient as well as patient interest. A lack of health literacy may lead to misinterpretation of health information, incorrect entry of data into the PHR or overwhelm the patient due to the large amounts of information displayed in the PHR. A lack of computer literacy would lead to issues regarding the utilisation of the PHR. Lastly, patient interest in the PHR is another challenge as interest would be low if patients did not find any value in using the PHR. Thus, these barriers to adoption would need to be addressed through patient education and by making the PHR more user friendly. Although Gagnon et al. (2016) discussed challenges pertaining to the PHR in their study, the same challenges would also apply to the EHR.

Sweden

In Sweden there has been limited support for patient participation with regards to their health records. According to Hägglund and Scandurra (2017), one of the expected benefits of the EHR is to increase patient participation in their healthcare. However, collaboration between patients and clinicians is required for this to happen and the Swedish EHR does not automatically enable this. It is important that patient participation is included in the development of the EHR since this will have an influence on the patient adoption of the EHR.

England

The use of the HealthSpace portal for viewing the patient's EHR has had a negative impact on the patient adoption of the EHR in England. Greenhalgh, Hinder, Stramer, Bratan, and Russell (2010) conducted a study that focussed on the adoption of HealthSpace since its introduction in 2007. The study found that many patients had abandoned the use of HealthSpace. The HealthSpace portal allowed patients to record health information such as blood pressure (using a basic account) and also view their SCR (using an advanced account). At the end of October 2010, only 0.13% (2913 out of 2 442 215 people in England who were invited to open a HealthSpace advanced account) had activated their HealthSpace account. Reasons for the low adoption of HealthSpace was due to limited patient interest and also because of a cumbersome registration process. The study of Greenhalgh et al. (2010) also indicated that the patients found HealthSpace of limited value, not easy to use and there were limited options for sharing information with their clinician. As a result of the low adoption, HealthSpace was closed in 2013 (De Lusignan & Seroussi, 2013). It is imperative that patients' feedback is incorporated into the EHR in order to mitigate the negative impact which barriers have on the use of the EHR. The third challenge, network connectivity problems, is discussed next.

3.5.3. Network Connectivity Problems

Network connectivity is essential for the realisation of a national EHR system. However, network connectivity problems will prevent the realisation of a national EHR system. Achieving interoperability (more specifically foundational interoperability as discussed in Chapter 6: Section 6.2.1) is dependent on systems that are connected together over the network (Ryan & Eklund, 2010). However, as discussed in this section, the examined countries have experienced network connectivity problems including bandwidth issues and no network being available which has negatively affected the implementation of the EHR. Network connectivity problems that have been experienced by Canada are covered below.

Canada

A lack of network connectivity acts as an inhibitor to the use of the EHR. In the study of Gagnon et al. (2016), it was identified that disadvantaged people may not have access to the internet. This would prevent them from utilising the PHR, which was the focus of the study. In addition to preventing the use of the PHR, this would also act as a barrier to the use of a national EHR and any other eHealth applications. Hence, this barrier should be addressed prior to the development of the EHR.

New Zealand

Deloitte (2015) mentions that there exists an issue with accessing datasets that are distributed across multiple systems. This is due to a large amount of latency which leads to delays in both the processing of data and network connectivity. This would cause delays in alerts from decision support systems such as EMR systems, which are supposed to run in real time. This would consequently negatively affect critical decisions that are made by clinicians and have a direct effect on their patients. Thus, network latency would need to be reduced through utilising robust networks with adequate bandwidth, which would allow EMR system alerts to be delivered in real time.

South Africa

Many parts of South Africa's nine provinces have been negatively affected by poor network connectivity. One example includes the Clinicom EMR system that is widely used in the Western Cape (Ohuabunwa et al., 2016). The aim was to implement a fully working EMR system in 38 different hospitals and specialised care centres in the Western Cape. However, this has been hindered due to the bandwidth requirements in health facilities which have not been met. As a result, the EMR systems at these health facilities will not be able to communicate at a regional level and consequently there will also be no interoperability between these EMR systems. Weeks (2014) states that technological concerns relating to network connectivity and bandwidth have an impact on the EMR systems which are implemented. This is true as without strong network connectivity and sufficient bandwidth the exchange of patient information will become degraded. Another problem that is acting as a barrier to a South African national EHR system is that there is no supporting network infrastructure in certain areas. This is due to the fact that computer and internet access is not a common occurrence in government hospitals or even at the provincial level (Department of Health South Africa, 2012). These networking components would need to be addressed before a national EHR system can be realised.

Sweden

Although many Swedish EMR systems are accessible nationally via the national HIE platform, EMR systems exist that are not connected. Hägglund and Scandurra (2017) state that this could be due to technical issues which result in the affected systems not being able to connect nationally. The consequence of this is that the patient's continuity of care will be affected whereby a patient moving between different regions may end up with parts of their information missing. To ensure that the patient's continuity of care is realised, unconnected regions should address the inherent technical issues in order to be able to connect to the national HIE platform.

England

Despite the growth of internet access in England, with the majority of people having broadband access to the internet, there exists a part of the English population who do not have internet access (Department of Health England, 2012). Additionally, those who do not have internet access are the part of the English population who would benefit most from the use of the EHR such as people with a low income. This has an impact on the patient adoption of the EHR due to the requirement of internet access to access the EHR. Thus, it is important that emphasis is placed on making internet access available to those who would need it in order to access the EHR. Next, the challenge of clinician resistance to EHR adoption is covered.

3.5.4. Clinician Resistance to Electronic Health Record Adoption

In this section, clinician resistance to the use of the EHR in each of the five countries is discussed, which also includes a discussion of the resistance to the EMR where a country has not yet reached the stage of a national EHR. This challenge includes a number of barriers that are discussed such as a lack of computer literacy and consultation. Clinician resistance with regards to Canada's adoption of EMR systems is discussed next.

Canada

The clinician adoption of EMR systems in Canada has faced a number of barriers. Chang and Gupta (2015) mention these barriers to adoption with a lack of computer literacy being the greatest barrier. Other barriers include the time needed to learn to use the EMR system and the amount of time spent capturing patient information into the EMR system. This may be seen as more work for the clinician but it is important that the EMR system is user friendly in order for clinicians to adopt it.

New Zealand

New Zealand has encountered problems with opening up doctors' consultation notes to patients. Opening up consultation notes to patients, via portals, has been seen as a challenge since this represents a major patient-provider relationship change (Wells, 2017). Doctors may not embrace this change since opening up consultation notes to patients may confuse or make patients anxious. This is because doctors' notes may contain obscure abbreviations and jargon which may be hard for patients to interpret on their own. As a result, this may lead to patients seeking clarification from doctors which can take up more of the doctor's time. The proposed model (Chapter 8: Section 8.6.4) discusses the use of a patient portal for granting patients access to certain sections of their EHR which would provide the patient with useful information such as the list of medication that they are on.

South Africa

South Africa has also encountered clinician resistance where the adoption of an EMR system experienced a number of problems. Ohuabunwa et al. (2016) mention that the adoption of the

Clinicom EMR system experienced challenges including a lack of computer literacy and motivation to correctly use the system. This resulted in resistance from clinicians who in addition to using the EMR system, also used paper-based records. Similarly, a Pretoria clinic also experienced several challenges relating to the clinician acceptance of EMRs, which resulted in the use of a dual system of EMRs and paper-based records. Weeks (2014) elaborates on this by mentioning that nurses at the clinic had been accustomed to paper-based records and this acted as a barrier which opposed the culture change of using EMRs. Additionally, nurses perceived the use of the EMR system as being more time consuming than paper-based records. Thus, the EMR system was seen as being a duplication of effort. This highlights the importance of involving clinicians during the development of the EMR system, which would help with the transition from paper-based records to EMR systems.

Sweden

There has been some resistance from clinicians in Sweden with regards to the idea of patients having access to their health information through the EHR. Hägglund and Scandurra (2017) mention that many have argued that the EHR puts the patient at risk and that certain information contained in the EHR needs to be blocked in order to protect the patient. For instance, while looking at their EHR a patient may find out that they have contracted a disease. Clinicians may feel that only they should communicate this information to the patient. As discussed earlier with New Zealand, instead of giving patients full access to the EHR, it would be better if patients are granted access to the sections of the EHR which would be useful to them.

England

The clinician adoption of England's EHR has experienced a number of problems. Brennan (2007) states that there was a false expectation about the attitude of the clinicians who would eventually use the EHR system. This false expectation was believed by the local service providers who envisioned that the clinicians would be receptive to the adoption of new systems as it would support their work. However, this belief was not supported by the clinicians. This is evident as Brennan (2007) reported that very few doctors had sufficient consultation regarding the NHS IT systems which resulted in decreased enthusiasm. This emphasises that no matter what benefit a new system may bring to clinicians, it will never be optimally utilised unless it is accepted by the clinicians. The clinician adoption of the EHR, in England, has also been influenced by systems which do not function correctly. For example, in 2014, Cambridge University Hospitals implemented an EMR system which experienced a number of issues

(Parliamentary Office of Science and Technology, 2016). This resulted in several system issues and a lack of training of clinicians which lead to clinicians reverting back to paper-based records. The fifth challenge, security and privacy issues, is discussed below.

3.5.5. Security and Privacy Issues

Security and privacy issues are a major challenge that needs to be addressed in order to protect patient information. The examined countries' security and privacy issues assists with addressing the research problem since these issues can serve as lessons learned so that they are not repeated in the implementation of the South African national EHR system. This section focuses on the security and privacy issues of the examined countries that range from data breaches of patient information to the illegal sharing of patient information without the patient's consent. The security and privacy issues that Canada has experienced with regards to the adoption of the PHR is covered below.

Canada

In Canada, the adoption of the PHR has been low and those which are in use are either not well known or are not widely used (Gagnon et al., 2016). In addition, there is no specific regulation regarding the PHR in Canada. This is not favourable as the security and privacy of patients' PHRs is at risk since there are no specific regulations to enforce the protection of the PHR. This emphasises that the security and privacy of patients' PHRs does not only depend on technical controls but also non-technical controls such as regulations.

New Zealand

In New Zealand, clinicians have found that current systems do not offer a secure way to exchange patient information (Deloitte, 2015). Due to the limitations of sharing information securely, clinicians have opted to printing out patient information which is later either scanned or faxed. Another means of exchanging patient information between clinicians includes moving information via USB flash drives and laptops. However, this creates a security and privacy risk since the loss of these items, containing patient information, exposes patient information to a data breach. Thus, access control would be needed to ensure that patient information is secured.

South Africa

In South Africa, there have been challenges regarding the security of EMR systems. Weeks (2014) mentions the case of a Pretoria clinic where the EMR system, which was implemented at the clinic, experienced challenges regarding confidentiality requirements which were still outstanding and had not been applied to the EMR system. Hence, it is imperative that the development of any EMR system considers security in order to reduce the risks to patient information stored in EMR systems.

Sweden

Requesting patient consent, in order to share information stored in a patient's EHR, should always be adhered to. However, Kierkegaard (2011) refers to an event where Sweden's data protection authority ruled in 2011 that Karolinska University Hospital failed to provide patients with the choice to opt-out of the sharing of their EHR information. As a result, Karolinska University Hospital violated the law. This was due to the Swedish Patient Data Act which states that the sharing of EHR information requires patient consent. Thus, it is important that the adopted consent model complies with regulations.

England

England's SCR has experienced several problems regarding the security and privacy of the SCR. De Lusignan and Seroussi (2013) state that the consent model of the SCR is an opt-out model. In the opt-out model a SCR is created for all English patients and it is up to the patient to decide whether they want their SCR to be unavailable on the centralised Spine. This would involve the patient submitting an application to prevent their SCR from being accessible. The opt-out model is disadvantageous from a security and privacy perspective since SCRs are created for all English patients, yet some patients may not want a SCR to be created and shared with parties without their consent. Coiera (2007) adds that patients need to be informed in advance about the consent model before the implementation of the system. This is important as patients need to give their consent in order for their confidential information to be stored in the system, which will be accessible to other parties. An opt-in model would be a viable option since it takes the patient's consent into consideration before adding their information to the system. England's NHS has also experienced other security and privacy issues in the form of data breaches. According to Big Brother Watch (as cited in Parliamentary Office of Science and Technology, 2016), 7255 cases of NHS data breaches have been reported between 2011 and 2014. This included cases where clinicians had wrongly accessed patient information or lost devices containing patient information. The challenge of governance issues is discussed next.

3.5.6. Governance Issues

Governance plays a key role in the realisation of a national EHR system. Governance is defined as the process of governing with the goal of providing strategic direction, ensuring the achievement of objectives and appropriate management of risks (Whitman & Mattord, 2016). The application of governance to the proposed model is covered in Chapter 8: Section 8.6.8. All of the examined countries experienced issues with governance that inhibited the adoption of the EHR. These governance issues created further challenges such as a lack of leadership and understanding as well as standardisation issues. Governance issues that hindered the adoption of EMR systems in Canada are discussed next.

Canada

The implementation of EMR systems within Canada have experienced governance-related problems. Chang and Gupta (2015) elaborate on this by mentioning that a lack of leadership and direction, in previous years, impeded many clinicians from adopting the EMR system. This highlights the importance of governance during the implementation of EMR systems as this will determine whether clinicians are more likely to accept the numerous changes which are made during the implementation of EMR systems.

New Zealand

New Zealand has encountered issues with regards to its governance structures. The use of a federated model for New Zealand's health system governance places emphasis on the local level and as a result inhibits regional collaboration and ultimately national standardisation (Deloitte, 2015). This is due to the autonomy of district health boards which has resulted in regional IT systems which vary greatly due to the use of disparate technologies. Thus, it is important that a national governance structure provides direction for the New Zealand regions to collaborate and to ensure national standardisation which will help realise a national EHR system.

South Africa

South Africa has experienced challenges due to a lack of governance in the public sector. There has been a lack of cooperation between numerous groups due to a lack of understanding that eHealth includes all ICTs for health such as the EHR (Department of Health South Africa, 2012). Consequently, this has resulted in the hindering of progress which could be made by using eHealth as an enabler. There have also been challenges experienced with regards to information governance which is needed in order to ensure compliance with essential standards such as interoperability standards and to also ensure that the use of patient information adheres to regulations.

Sweden

The decisions made by those who oversee the implementation of the EHR has an impact on the end users such as clinicians. This is supported by Janols, Lind, Göransson, and Sandblad (2014) who refer to a hospital, in one of Sweden's counties, where a Patient Administration System (PAS) was deployed. The managers had delegated the responsibilities for the deployment process to a group of superusers (who represented several wards) and some of the managers had a different perception of how involved they needed to be. Consequently, there were managers who did not take part in learning sessions, stating that they were not going to be the end users of the system. As a result, the PAS was not utilised as planned since the PAS was not considered to be important by the end users. This emphasises that the actions made by governance structures has an impact on the clinician adoption of the EHR.

England

The English governance structure for the NPfIT has had misunderstandings with the content of the NPfIT i.e. programme. Brennan (2007) mentions that there was a lack of understanding regarding the content of the NPfIT by those at a senior level in the programme and government. Electronic transmission of prescriptions, which was part of the programme, was confused with electronic prescribing, which was not part of the programme. This misunderstanding was later acknowledged by the NPfIT board. This emphasises that governance structures must have a good understanding of the programme in order to ensure that there are no misunderstandings which would later affect the implementation of the systems. Lack of interoperability, which is the seventh challenge, is covered below.

3.5.7. Lack of Interoperability

A lack of interoperability is a difficult challenge that needs to be addressed in order for a national EHR system to be realised. As discussed below, a lack of interoperability has affected all of the examined countries. A lack of interoperability is due to a number of reasons including three of the previously discussed challenges: concurrent use of paper and EHRs, network connectivity problems and governance issues. Most notably from the discussion of the examined countries, the use of disparate systems has also created a lack of interoperability. Canada's experience of a lack of interoperability with regards to its provincial systems is covered below.

Canada

Canada's EMR systems have not reached the stage where they can all communicate and exchange patient information with each other. This is due to a lack of interoperability between systems which has inhibited the adoption of the EMR (Chang & Gupta, 2015). This is attributed to the variation in provincial systems which has been a result of provinces implementing EMR systems from different vendors. Thus, it is important that disparate systems can interface with each other so that interoperability can be realised.

New Zealand

New Zealand's EMR systems have also experienced the issue of a lack of interoperability between systems. This has caused hospital systems to be fragmented with most hospitals running hundreds of different health information systems (Deloitte, 2015). As a result, processes which have already been automated, such as eReferrals, have to be re-entered into those EMR systems which cannot receive this information from other systems. This results in extra work for clinicians and can lead to errors when the information is re-entered by hand. To avoid these errors, it is important that the interoperability issues are addressed otherwise clinicians will continue to work using manual processes.

South Africa

There has been a lack of interoperability between the provincial systems in South Africa which has led to disparate systems which cannot communicate with one another (Department of Health South Africa, 2012). These proprietary systems have been implemented using different platforms and databases and differ in terms of their architecture and usability. The private sector also faces the same interoperability problems as the public sector. The issue of a lack of interoperability is made more complex since many hospitals rely solely on paper-based records. Thus, interoperable EMR systems should be used instead of paper-based records to ensure that interoperability can be achieved.

Sweden

Although Sweden uses a national HIE platform to exchange information between disparate systems, some hospitals have experienced problems with regards to interoperability. Rexhepi et al. (2015) refer to a hospital in the region of Västra Götaland that suffered from a lack of interoperability in its information systems. As a result, before a clinician saw a patient, the clinician had to navigate through all the information systems to obtain an overview of the patient's medical history. At the same time, the clinician found that some of the patient's information was missing. Another problem is unstructured information in the EHR which does not comply with standards. Rexhepi et al. (2015) also mention that since information in the EHR is recorded as free text, without any format, it takes a large amount of time to review manually. This has been experienced by clinicians who have had difficulties with extracting information. Thus, it is imperative that the structure of the EHR complies with standards to ensure that it can be interpreted and that it is also interoperable with other systems.

England

A lack of interoperability has also affected England's health information systems. One event of this occurring was due to integrations that were needed to ensure interoperability but were never included during procurement (Brennan, 2007). One NHS trust would buy a system for a hospital, while primary care would also buy their own systems resulting in a myriad of fragmented systems being used. Consequently, this did not support the patient journey which requires that all systems are interoperable in order to access the complete medical history of the patient. The final challenge, lack of technical support, is discussed next.

3.5.8. Lack of Technical Support

Technical support has an important role in ensuring that the EHR is adopted by both clinicians and patients. However, as discussed below, the examined countries have experienced issues with the adoption of the EHR due to a lack of technical support. The reasons for the lack of technical support include a lack of knowledgeable support personnel, varying support structures as well as the assumption that technical support is not needed. From the five examined countries, New Zealand did not have the required information for this challenge. A lack of technical support in the Canadian context is discussed next.

Canada

Technical support plays a key role in the adoption of the EMR by clinicians both during implementation and post implementation. Without sufficient technical support, this can have a negative impact on the adoption of the EMR. This has been the case with the utilisation of Canada's regional EMR systems by clinicians. Chang and Gupta (2015) elaborate on this by stating that the inhibitors to the adoption of the EMR include a lack of knowledgeable support personnel. Thus, it is important to have technical support in place which can support EMR systems as opposed to generic IT systems.

South Africa

South Africa's aim of achieving a national EHR has been affected due to the emergence of varying support structures (Department of Health South Africa, 2012). This has been caused by the fact that a variety of proprietary systems have been implemented in South Africa's nine provinces. Since each proprietary system comes with its own unique support structure, this will result in different support structures throughout the country. Thus, clinicians moving between hospitals may not receive the same level of technical support compared to what they would receive in other hospitals. Hence, it is important that the number of vendors is kept to a minimum as this will also reduce the variety of support structures.

Sweden

Sweden has experienced some problems with regards to the use of eHealth systems including EMR systems. One of the reasons is attributed to a lack of technical support. Öberg et al. (2018) mention an example where nurses had complained due to a lack of training and technical support on the use of new eHealth systems. Thus, it is essential that technical support is made available to clinicians so that their job functions are not inhibited while using eHealth systems.

England

England has also faced some implementation problems due to a lack of technical support. Greenhalgh et al. (2010) mention that English policy makers treated HealthSpace, the portal for accessing the EHR, as a 'log on and play' technology. Additionally, it was assumed that future end users would not require training and technical support to use it. As discussed in Section 3.5.2, the end users found HealthSpace difficult to use and subsequently abandoned using it. This highlights the importance of incorporating technical support in order to ensure that the EHR can be used by all end users. The summary of this chapter is covered next.

3.6. Summary

This chapter discussed national EHR adoption internationally by five countries: Canada, New Zealand, South Africa, Sweden and England. Firstly, the three types of health records: the EMR, EHR and PHR were explained including how one health record may comprise of another. The current state of the examined countries' national EHR systems was then discussed, highlighting that some countries are at an advanced stage, while other countries are still at the planning stage and may only have a conceptual national EHR. Next, the centralised and distributed system architectures were examined, including their advantages and disadvantages. This was followed by the discussion of the national EHR system architectures

Table 3.4: Summary of challenges experienced by examined countries during national electronic health record implementations

Challenges	Canada	New Zealand	South Africa	Sweden	England
Concurrent use of paper and EHRs	EMR systems used in combination with paper-based records				
Lack of patient adoption of EHRs	Barriers: health and computer literacy, patient interest	*	*	Patient participation in EHR limited	Limited patient interest and difficulty in using EHR
Network connectivity problems	Internet access barrier	Network latency: delays in EMR alerts	Poor bandwidth	Some EMR systems not accessible nationally	Internet access barrier
Clinician resistance to EHR adoption	Lack of computer literacy	Resistance giving patients access to EHR	Lack of computer literacy and motivation	Resistance giving patients access to EHR	Little consultation with clinicians
Security and privacy issues	Lack of PHR regulation	Insecure exchange of patient information	Outstanding confidentiality requirements	Patient consent not requested	Data breach of patient information
Governance issues	Lack of leadership	Regional collaboration inhibited	Lack of cooperation and understanding of eHealth	Managers not involved in deployment of patient administration system	Misunderstanding with national EHR programme content
Lack of interoperability	Fragmented health information systems not interoperable				
Lack of technical support	Lack of knowedgeable support personnel	*	Varying support structures	Lack of training and technical support	Lack of training and technical support

Compiled from: (Brennan, 2007; Chang & Gupta, 2015; Deloitte, 2015; Department of Health England, 2012; Department of Health South Africa, 2012; Gagnon et al., 2016; Greenhalgh et al., 2010; Hägglund & Scandurra, 2017; Janols et al., 2014; Kierkegaard, 2011; Öberg et al., 2018; Ohuabunwa et al., 2016; Parliamentary Office of Science and Technology, 2016; Rexhepi et al., 2015; Weeks, 2014; Wells, 2017)

* No information available

that were used by the examined countries. Finally, a number of challenges regarding the national EHR implementations were covered for each of the examined countries. Examining these challenges served as lessons learned, which can be used by the future implementation of the South African national EHR system so that the same mistakes are not repeated. Additionally, where a country was still in the early stages of its national EHR programme and did not have an interoperable EHR, these challenges were discussed in terms of the EMR systems which were implemented and serve as the foundation for the national EHR. The next chapter covers the regulations that are needed for a compliant national EHR system.

CHAPTER 4: REGULATIONS FOR A COMPLIANT NATIONAL ELECTRONIC HEALTH RECORD SYSTEM

4.1. Introduction

This chapter discusses regulations that regulate the processing of personal information in order to ensure that it is protected. Regulations assist with addressing the research problem since access control, which can be used to protect patient information, is informed by regulations. The examined regulations comprise of those countries which were covered in the previous chapter: Canada, New Zealand, South Africa, Sweden and England. Also included in the examined regulations is the Health Insurance Portability and Accountability Act (HIPAA) of the United States (US), the Data Protection Directive and the General Data Protection Regulation (GDPR) of the European Union (EU). The examined regulations are also compared with South Africa's PoPI Act principles. This is followed by a discussion of the characteristics of regulations. Lastly, the chapter covers the security and privacy standards that can be used to aid compliance with regulations. The regulations that inform the use of a national EHR system are discussed below.

4.2. Regulations Informing the Use of a National Electronic Health Record System

In this section, a number of regulations are discussed that focus on the protection of personal information. These regulations include the countries which were covered in Chapter 3: Canada, New Zealand, South Africa, Sweden and England. It was important to cover the regulations of these countries since the countries' national EHR system architectures were discussed in Chapter 3: Section 3.4.3. Additionally, a discussion of the US's HIPAA has been included in this chapter. HIPAA was included since the results of the content analysis, in Chapter 7: Section 7.2.2, indicated that HIPAA was the most tagged regulation. Also discussed in this section is the Data Protection Directive and the GDPR. Both of these regulations were important to include since they have influenced some of the examined countries' national regulations. The next section begins with a discussion of the Data Protection Directive.

4.2.1. Data Protection Directive (European Union)

In 1995, the Data Protection Directive (also known as Directive 95/46/EC) was adopted by the EU with the aim of regulating the processing and transfer of EU citizens' personal information (Tikkinen-Piri, Rohunen, & Markkula, 2018). The Directive, including its important principles, has been implemented by EU member states through their national regulation(s) (DLA Piper, 2018). While these national regulations have originated from the Directive, there is great variation in the EU member states' national regulations. However, this variation has been addressed through the implementation of the GDPR (discussed in the next section) across all EU member states. Although the Directive has been the central instrument for EU data protection since its adoption in 1995, it has experienced a number of disadvantages (Tikkinen-Piri et al., 2018). One main disadvantage is that the Directive does not meet the privacy requirements of the present technological age. This is because the Directive was adopted to regulate technologies which were used for processing information in the 1990s. However, current technologies process larger amounts of information which may not be adequately regulated by the Directive. Robinson, Graux, Botterman, and Valeri (2009) elaborate on this by stating that the Directive is outdated with regards to technology and regulatory approach. Some other disadvantages mentioned include inadequate focus on loss, risk and practical enforcement, its scope is not clear and the Directive focusses on 'how' organisations should do things rather than 'what' they should be doing. In spite of the disadvantages, Robinson et al. (2009) mention a number of advantages of the Directive. The Directive is technology neutral, allowing organisations to implement a technology of their choosing that will comply with regulations. It has also given EU citizens important rights regarding data protection. Thirdly, the Directive has served as a reference model for good practice with other countries' regulations being created based on the Directive. This includes South Africa's PoPI Act, which is covered in Section 4.2.3. The GDPR, which has replaced the Data Protection Directive, is discussed below.

4.2.2. General Data Protection Regulation (European Union)

The GDPR, implemented in 2018, aims to improve the data protection of EU citizens (Tikkinen-Piri et al., 2018). This is ensured through clarified rules, clearly defined requirements and direct instructions as specified in the regulation. These improvements will address the various disadvantages of the Data Protection Directive, which were mentioned in the previous section. Although the GDPR aims to improve the data protection of EU citizens, there exists a big challenge with its implementation where there is a lack of awareness of the changes and requirements imposed by the GDPR. According to TRUSTe (as cited in Tikkinen-Piri et al., 2018), less than half of the organisations were aware of the changes enforced by the GDPR. Thus, in order to comply with the GDPR, it is important that these organisations are aware of the changes that are required. Unlike the Data Protection Directive where EU member states implemented the Directive through their national regulation(s), this is not the case with the GDPR (DLA Piper, 2018). As a result, the GDPR is directly applicable throughout the EU.

Similar to the Data Protection Directive, the GDPR is also based on data protection principles. However, the GDPR's principles have replaced the principles of the Data Protection Directive. Next, South Africa's PoPI Act is covered.

4.2.3. Protection of Personal Information Act (South Africa)

South Africa's PoPI Act, enacted in 2013, aims to promote the protection of personal information that is processed by both public and private organisations (DLA Piper, 2018). The PoPI Act aims to protect personal information through the use of minimum requirements for the processing of personal information. The protection of personal information is achieved by complying with the eight principles of the PoPI Act as indicated in Table 4.1. The PoPI Act is based on the Data Protection Directive (Botha, Eloff, & Swart, 2015). Consequently, the PoPI Act's eight principles are similar to the data protection principles of the Data Protection Directive. At present only some sections of the PoPI Act have come into effect (DLA Piper, 2018). It is anticipated that the remaining sections of the PoPI Act will come into effect in 2018. With regards to PoPI compliance, a survey conducted by Cibecs (as cited in Botha et al., 2015) found that only 40% of South African organisations are in the process of complying with the PoPI Act. This small percentage is due to a lack of awareness and understanding of the PoPI Act, which is required in order to be compliant with the PoPI Act's requirements. The next section discusses the US's HIPAA.

4.2.4. Health Insurance Portability and Accountability Act (United States)

The US's HIPAA was enacted in 1996 due to the need for increased protection of patients' information from unauthorised use and disclosure (Breaux & Antón, 2008). HIPAA aims to achieve this by regulating covered entities (DLA Piper, 2018). Covered entities refer to entities that process protected health information i.e. patient information such as healthcare providers. In addition to healthcare providers, HIPAA also regulates those who process patient information on behalf of covered entities such as service providers. Although HIPAA aims to protect patients' information by regulating covered entities and those processing patient information on behalf of covered entities, it has been outdated. Terry (2017) elaborates on this by stating that HIPAA was tailored to healthcare of the 1990s. As a result, HIPAA does not offer similar levels of protection compared to current regulations. In agreement, Terry (2017) states that HIPAA provides weaker protection than the GDPR. This is evident as the GDPR is a more recent and comprehensive regulation as opposed to HIPAA. Next, the UK's Data Protection Act (DPA) is covered.

4.2.5. Data Protection Act (United Kingdom)

The DPA of 2018 regulates the processing of UK citizens' personal information (Data Protection Act, 2018). With regards to the scope of the DPA, it covers both public and private organisations that process personal information. Similar to the GDPR, the DPA is also based on a number of data protection principles that specify the requirements for the protection of personal information. This is because the DPA was updated in order to be aligned with the GDPR (Data Protection Act, 2018). Previously, the UK implemented the Data Protection Directive via the DPA of 1998 (DLA Piper, 2018). However, the DPA of 1998 was replaced with the DPA of 2018 as a result of the GDPR superseding the Data Protection Directive. Sweden's Personal Data Act (PDA) is discussed below.

4.2.6. Personal Data Act (Sweden)

The PDA was enforced in 1998 in order to protect the personal information of Swedish citizens (Ministry of Justice, 2006). The PDA aims to ensure this by controlling the processing of personal information. Similar to how UK's DPA was implemented, Sweden implemented the Data Protection Directive through the PDA (DLA Piper, 2018). However, since the Data Protection Directive has been superseded by the GDPR, Sweden will need to comply with the GDPR as the PDA of 1998 is outdated in comparison to the GDPR. New Zealand's Privacy Act is discussed in the next section.

4.2.7. Privacy Act (New Zealand)

The Privacy Act of 1993 regulates how agencies process personal information of New Zealand citizens (DLA Piper, 2018). In the context of the Privacy Act, an agency includes a person or organisation operating in either the public or private sector. The Privacy Act contains twelve information privacy principles which agencies must comply with in order to ensure that New Zealand citizens' personal information is protected (Law Commission, 2010). These information privacy principles achieve this by setting out how and when agencies can collect, store, use and disclose personal information. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which is the final regulation that is covered in this chapter, is discussed below.

4.2.8. Personal Information Protection and Electronic Documents Act (Canada)

Canada's PIPEDA, enforced in 2004, controls the collection, use or disclosure of personal information that is carried out by private sector organisations via commercial activities (Peekhaus, 2008). Although PIPEDA's scope focuses on commercial activities that are run by private sector organisations, these commercial activities can include the processing of health information by health facilities which operate in the private sector. One of the reasons for enacting PIPEDA was due to international pressure that Canada received from the EU (Peekhaus, 2008). This occurred since prior to PIPEDA, Canada required a regulation that matched the EU's Data Protection Directive in terms of the protection of personal information. This was required in order to allow the transfer of personal information from the EU to Canada. PIPEDA includes ten fair information principles which determine how personal information is collected, used and disclosed while also enabling access to personal information (Office of the Privacy Commissioner of Canada, 2015). The aim of these principles is to control how private sector organisations handle personal information. Next, the examined regulations are compared against the eight PoPI Act principles.

4.3. Comparison of Regulations against PoPI Act Principles

This section compares the regulations, which were discussed previously, with the eight PoPI Act principles. The PoPI Act was the basis for comparison since this would be the most relevant regulation for protecting personal information in the context of a South African national EHR system. Table 4.1 describes each of the eight PoPI Act principles while also showing how they compare with other regulations. As depicted in Table 4.1, convergence exists between the eight PoPI Act principles and the examined regulations. A majority of the examined regulations are based on a number of data protection principles. These regulations (Directive 95/46/EC, DPA, GDPR, PIPEDA and the Privacy Act) contain sections that outline the purpose of each principle. These principles are similar to the principles of the PoPI Act. On the other hand, although the remainder of the examined regulations (HIPAA and PDA) do not contain sections outlining a number of data protection principles, the content of these regulations do overlap with the eight principles of the PoPI Act. The creation of the PoPI Act was based on Directive 95/46/EC (Botha et al., 2015). This is evident since the PoPI Act's principles are aligned with Directive 95/46/EC. The next section discusses the characteristics of the discussed regulations.

4.4. Characteristics of Regulations

This section examines characteristics of regulations that are relevant to the regulation of a national EHR system. These characteristics consist of processing, security, data protection authority, data protection officer, data breach notification and enforcement. While all of these characteristics are important to ensure a compliant national EHR system, emphasis is placed

Table 4.1: Comparison of regulations against PoPI Act principles

PoPI Act (South Africa) Principles	Description	Directive 95/46/EC (EU)	DPA (UK)	GDPR (EU)	HIPAA (US)	PDA (Sweden)	PIPEDA (Canada)	Privacy Act (New Zealand)
Accountability	Eight principles for lawful processing of personal information must be complied with	✓	✓	✓	✓	✓	✓	✓
Processing limitation	Limits must be placed on the processing of personal information	✓	✓	✓	✓	✓	✓	✓
Purpose specification	Collection of personal information must be done for a specific and lawful purpose	✓	✓	✓	✓	✓	✓	✓
Further processing limitation	Further processing of personal information must be compatible with original purpose for which information was collected	✓	✓	✓	✓	✓	✓	✓
Information quality	Collected personal information must be complete, accurate, not misleading and up to date	✓	✓	✓	✓	✓	✓	✓
Openness	Responsible party must be open by notifying Information Regulator before processing personal information. Subject must also be notified about processing	✓	✓	✓	✓	✓	✓	✓
Security safeguards	Confidentiality and integrity of personal information must be ensured through technical and organisational controls	✓	✓	✓	✓	✓	✓	✓
Data subject participation	Subject has right to request their personal information, which is held by responsible party, as well as its correction	✓	✓	✓	✓	✓	✓	✓

Compiled from: (Birnhack, 2008; Botha et al., 2015, Data Protection Act, 2018; Directive 95/46/EC, 1995; DLA Piper, 2018; Eisenberg, 2001; GDPR, 2016; Office of the Privacy Commissioner of Canada, 2015; PoPI Act, 2013; Privacy Act, 1993; Svensson & Advokatbyrå, 2018) on the security characteristic as the implementation of access control depends on this characteristic (access control is covered in detail in the next chapter). Firstly, the processing characteristic is covered below.

4.4.1. Processing

The processing of information is defined as the collection, recording and storage of information and includes the execution of operations on information (Information Commissioner's Office, 2018). These operations include the modification and disclosure of information. Most of the examined regulations refer to two entities which process personal information: the data controller and data processor. A data controller is a person or one or more organisations who jointly decide on the purpose and way in which personal information is processed (Information Commissioner's Office, 2018). On the other hand, a data processor is a person or organisation that processes personal information on behalf of the data controller. While the focus of the Data Protection Directive was on regulating data controllers, this focus has shifted with the implementation of the GDPR (DLA Piper, 2018). Consequently, data processors are now directly regulated by the GDPR. This is an essential change as data processors who process personal information are now regulated in the EU while in the past the data controller was responsible for this processing. As mentioned earlier, Sweden and the UK (DPA of 1998) are two countries who implemented the Data Protection Directive via their national regulations. Thus, data processors were not directly regulated by these national regulations (Information Commissioner's Office, 2018; Ministry of Justice, 2006). However, with the enforcement of the GDPR, data processors are now regulated in these two countries along with the other countries in the EU (DLA Piper, 2018).

In order for the processing of personal information to be legitimate, it must comply with a number of conditions. Firstly, personal information must be collected for a specific, explicit and legitimate purpose and the processing of this information must be done in a lawful manner. For instance, with regards to a national EHR, the main purpose for collecting personal information is to provide improved healthcare through the use of a national EHR. Additionally, the processing of information would be lawful if the reason for EHR access during an emergency is to treat the patient. It is also important that patients are provided with the option to consent to the processing of their personal information as a result of using the EHR. Secondly, limitations must be placed on the processing of personal information. This comprises of collecting personal information that is not excessive and is relevant with regards to the specific purpose for which it is processed. This is referred to as 'data minimisation' since the collection of personal information is kept to a minimum while still fulfilling the original purpose. For example, requiring a patient to provide their political opinion is excessive and not relevant with regards to the purpose of providing improved healthcare. Thirdly, personal information should not be further processed in any way that is incompatible with the original purpose for which it was collected. However, the further processing limitation does not apply if the personal information is anonymised. For instance, anonymised health information from a patient's EHR can be used for research or statistical purposes (Birnhack, 2008; Data Protection Act, 2018; Directive 95/46/EC, 1995; DLA Piper, 2018; Eisenberg, 2001; GDPR, 2016; Office of the Privacy Commissioner of Canada, 2015; PoPI Act, 2013; Privacy Act, 1993; Svensson & Advokatbyrå, 2018). Security, which is an essential characteristic of regulations, is discussed next.

4.4.2. Security

Security is an important characteristic of regulations as it specifies that personal information should be protected from threats through the use of technical and organisational controls i.e. security controls (Data Protection Act, 2018; Directive 95/46/EC, 1995; DLA Piper, 2018; GDPR, 2016; Office of the Privacy Commissioner of Canada, 2015; PoPI Act, 2013; Privacy Act, 1993; Svensson & Advokatbyrå, 2018). These threats include unauthorised access, modification or disclosure of personal information as well as the accidental loss of information. Thus, security controls need to be implemented in order to reduce the risks to information which are created by these threats. As a result, this will ensure that only authorised entities are allowed to access, modify or disclose personal information, as long as regulations are complied with. It is also important that personal information is protected irrespective of what form it may be in. For example, in a national EHR system, patient information may either be stored or transferred. Patient information may be stored in the EMR, which is located in different health facilities. Whenever access to an EHR is requested, the personal information would need to be transferred to the location where the EHR is requested. Hence, both the storage and transfer of personal information need to be protected by using relevant security controls. It is important to note that while the examined regulations specify the protection of personal information using security controls, they do not specify the type of technologies that should be used. Thus, it is up to the data controller to decide on the types of technologies that will be used. It is also essential that security controls are periodically evaluated in order to ensure that they are effective and up to date.

The GDPR introduces two concepts of 'data protection by design and by default', which have an influence on how security controls should be implemented (GDPR, 2016). Data protection by design (also known as privacy by design) requires that the implementation of security controls is integrated with processing. This ensures that security controls are implemented from the start and not after processing, which will ensure that processing complies with the GDPR. The second concept of data protection by default requires that implemented security controls ensure that only personal information necessary for a specific purpose is processed. Data protection by default also ensures that limitations are placed on the collection, processing and storage of personal information while also restricting access to personal information. Additionally, it is also important that the implemented security controls are designed to implement data protection principles such as data minimisation. Data protection authority, which is the third characteristic of regulations, is discussed below.

4.4.3. Data Protection Authority

A data protection authority is an authority that monitors and enforces compliance with regulations (GDPR, 2016). This is the main task of a data protection authority and involves regulating how organisations process personal information with the aim of protecting individuals' personal information such as patient information. A data protection authority also handles complaints and can investigate these complaints and inform the complainant on the status of the investigation. These investigations can also be carried out in the form of security audits. A data protection authority can also impose sanctions on a non-compliant organisation. Additionally, a data protection authority may instruct organisations to notify affected individuals of any data breaches which may have affected them. For example, a hospital would be obliged to notify patients if they have been affected by a data breach. However, data breach notifications may not be mandatory and it depends on whether the country's regulations enforce this. Next, the role of the data protection officer is covered.

4.4.4. Data Protection Officer

A data protection officer is a role within an organisation that is responsible for the protection of individuals' personal information including patient information (Nieuwesteeg, 2016). Similar to a data protection authority, a data protection officer has a number of tasks relating to the protection of personal information (Tikkinen-Piri et al., 2018). These tasks include monitoring organisations' compliance with regulations. The data protection officer also has the responsibility of training staff who are involved with the processing of personal information. Those involved with the processing of personal information would include clinicians who have access to patients' EHRs. Another important responsibility of the data protection officer is to function as a contact point for the data protection authority. As depicted in Table 4.2, the role of the data protection officer is not mandatory in all of the examined regulations. However, despite not being mandatory in some regulations, it is an important role for ensuring the protection of personal information. Data breach notifications are discussed in the next section.

4.4.5. Data Breach Notification

A data breach notification consists of notifying the data protection authority and affected individuals about a breach of personal information (Tikkinen-Piri et al., 2018). This breach of personal information, i.e. data breach, involves unauthorised access, disclosure or loss of personal information. The Law Commission (2010) mention a number of justifications for the use of data breach notifications. Most importantly, notifying affected individuals of the occurrence of a data breach allows them to take steps to mitigate any damage caused by the data breach. For example, in the context of a comprised EHR, an affected patient can change the password of their EHR account and could also monitor the EHR audit trail for any suspicious activity using a user-friendly interface. Despite this justification, data breach notifications are not mandatory in a number of countries. Table 4.2 indicates those examined regulations where data breach notifications are mandatory and not mandatory. The two regulation characteristics of security and data breach notification are linked. In all the examined regulations, an organisation has the responsibility to ensure the security of personal information. A data breach often occurs when the organisation fails to ensure the security of personal information. Thus, data breach notifications should be a mandatory requirement as the organisation has failed to secure the personal information of individuals. Enforcement, consisting of the consequences for non-compliance with regulations, is covered below.

4.4.6. Enforcement

The enforcement of regulations is essential in order to ensure compliance with the rules contained in regulations. The enforcement process consists of conducting investigations that can lead to the implementation of sanctions on non-compliant organisations (DLA Piper, 2018). An investigation is conducted by the data protection authority upon being informed of a non-compliant organisation. An organisation that has been found to be in breach of the regulation can be given an enforcement notice by the data protection authority to rectify the situation. Failure to comply with the enforcement notice can lead to sanctions being imposed in the form of fines and imprisonment. The magnitude of the imposed sanctions vary from country to country. In addition to enforcing sanctions on a non-compliant organisation, the organisation can also experience reputational damage. For instance, a data breach due to non-compliance with a regulation's security rules can lead to the reputational damage of an organisation's image. In the context of a national EHR system, a data breach of patient information can cause reputational damage to the affected health facility's image, which could ultimately result in patients losing trust in the national EHR system. The next section covers security and privacy standards which can help with the compliance of regulations.

Table 4.2: Characteristics of regulations

Characteristic	**Directive 95/46/EC (EU)**	**DPA (UK)**	**GDPR (EU)**	**HIPAA (US)**	**PDA (Sweden)**	**PIPEDA (Canada)**	**PoPI Act (South Africa)**	**Privacy Act (New Zealand)**
Processing	✓	✓	✓	✓	✓	✓	✓	✓
Security	✓	✓	✓	✓	✓	✓	✓	✓
Data protection authority	✓	✓	✓	✓	✓	✓	✓	✓
Data protection officer		✓	✓	✓		✓	✓	✓
Data breach notification		✓	✓	✓		✓	✓	
Enforcement	✓	✓	✓	✓	✓	✓	✓	✓

Compiled from: (Brown, 2018; Data Protection Act, 2018; Directive 95/46/EC, 1995; DLA Piper, 2018; GDPR, 2016; Office of the Privacy Commissioner of Canada, 2015; PoPI Act, 2013; Privacy Act, 1993; Svensson & Advokatbyrå, 2018; Terry, 2017)

4.5. Security and Privacy Standards for Aiding Compliance

Up until now, the examined countries' regulations and their characteristics have been discussed. This discussion comprised of what is required in order to ensure compliance with regulations. In addition to these regulations, security and privacy standards exist that can assist with compliance. Two important standards that will be covered include the ISO/IEC 29100 privacy framework and the ISO/IEC 27001 information security management system standards. This section begins with the discussion of the ISO/IEC 29100 privacy framework below.

4.5.1. ISO/IEC 29100 Privacy Framework

ISO/IEC 29100 is a privacy standard that provides a privacy framework in order to protect Personally Identifiable Information (PII) stored in ICT systems (ISO/IEC 29100, 2011). In the context of a national EHR system, PII refers to the personal information of patients while ICT systems comprise of those systems which make up the national EHR system. Thus, ISO/IEC 29100 can be applied to the context of a national EHR system in order to protect patients' EHRs, which are stored across a number of EMR systems. ISO/IEC 29100 aims to improve existing security standards by focussing on the processing of personal information. Hence, ISO/IEC 29100 is aligned with the examined regulations since it also focuses on the processing of personal information. This is depicted in the privacy framework's eleven privacy principles (Table 4.3) which are similar to the privacy principles of the examined regulations. This similarity is emphasised by Hoepman (2013), who states that the ISO/IEC 29100 privacy principles lie between legal requirements and privacy design strategies. Consequently, the concept of 'privacy by design' can be ensured by implementing the ISO/IEC 29100 privacy principles at the design stage of a national EHR system. Table 4.3 also shows the mapping of the ISO/IEC 29100 privacy principles to the principles of South Africa's PoPI Act. Thus, the mapping shows an alignment between ISO/IEC 29100 and the PoPI Act. Next, the ISO/IEC 27001 security standard is discussed.

Table 4.3: ISO/IEC 29100 privacy principles to PoPI principles mappings - compiled from (ISO/IEC 29100, 2011; PoPI Act, 2013)

ISO/IEC 29100 Privacy Principles	PoPI Act Principles
Consent and choice	Processing limitation
Purpose legitimacy and specification	Purpose specification
Collection limitation	Processing limitation
Data minimisation	Processing limitation
Use, retention and disclosure limitation	Further processing limitation
Accuracy and quality	Information quality
Openness, transparency and notice	Openess
Individual participation and access	Data subject participation
Accountability	Accountability
Information security	Security safeguards
Privacy compliance	Accountability

4.5.2. ISO/IEC 27001 Information Security Management System

The ISO/IEC 27001 security standard indicates the requirements for the establishment, implementation, maintenance and the improvement of an information security management system in an organisation (ISO/IEC 27001, 2013). In the context of this study, an organisation would refer to those organisations that process patients' personal information such as health facilities. Also included in ISO/IEC 27001 are the requirements for assessing and treating information security risks, which are specific to an organisation's needs. For example, the use of a national EHR within a health facility, providing access to a number of parties, could create risks to patients' information. Through the implementation of an information security management system within a health facility, a risk management process can be applied that will ensure that risks to patients' information are mitigated. As a result, the confidentiality, integrity and availability of information can be ensured. ISO/IEC 27001 (2013) also emphasises the importance of integrating the information security management system with an organisation's processes and governance structure. This also emphasises the inclusion of information security into the design of processes, controls and information systems. Thus, similar to the ISO/IEC 29100 privacy framework, ISO/IEC 27001 can also help ensure privacy by design.

The reduction of risks to personal information is attained through the implementation of security controls. ISO/IEC 27001 includes an array of security controls which consist of both technical and organisational controls (Coetzer, 2015). These security controls are also categorised under a number of control areas. Each control area comprises of control objectives, which are security goals in the form of statements. These control objectives are achieved through the implementation of relevant controls.

Table 4.4: ISO/IEC 27001 control areas relevant to access control - compiled from (ISO/IEC 27001, 2013)

Section	Control Area
A.5	**Information security policies**
A.6	Organisation of information security (A.6.1.2 **Separation of duties**)
A.9	**Access control**
A.12	Operations security (A.12.4 **Logging and monitoring**)
A.18	**Compliance**

Table 4.4 indicates the control areas which are relevant to this study regarding access control: both information security policies and compliance inform access control while operations security is also included as it comprises of logging and monitoring which ensure accountability (as discussed in Chapter 5: Section 5.7). Additionally, separation of duties is also relevant to this study as it forms part of the theoretical foundation: ANSI RBAC standards and the Clark-

Wilson model, which are discussed in Chapter 5: Sections 5.5 and 5.6.4 respectively. Security controls pertaining to access control are covered in more detail in the next chapter. This chapter is summarised in the next section.

4.6. Summary

In this chapter, a number of regulations were discussed that aim to protect personal information. The discussion included the regulations of countries that were covered in Chapter 3: Canada, New Zealand, South Africa, Sweden and England. In addition to the discussion of these countries' regulations, the following regulations were also covered: HIPAA, Data Protection Directive and the GDPR. Next, these regulations were compared against South Africa's PoPI Act principles, which indicated convergence. The following characteristics of regulations were then examined: processing, security, data protection authority, data protection officer, data breach notification and enforcement. Finally, two important security and privacy standards, which can be used to aid compliance with regulations, were covered: the ISO/IEC 29100 privacy framework and ISO/IEC 27001 information security management system standards. In addition to these standards, regulations such as the PoPI Act are essential for the protection of patient information within a South African national EHR system since regulations inform access control, which can be used to protect patient information. The next chapter covers securing the EHR through access control.

CHAPTER 5: SECURING THE ELECTRONIC HEALTH RECORD THROUGH ACCESS CONTROL

5.1. Introduction

In this chapter, the use of access control for securing the EHR is covered in terms of identification, authentication, authorisation and accountability i.e. IAAA. Access control relies on each component of the IAAA (Whitman & Mattord, 2016). Access control can be used to address the security and privacy aspects of the research problem, which were discussed in Chapter 1: Section 1.2. This chapter begins with identification and is followed by authentication including various authentication methods that are used to authenticate entities. Next, a number of access control models are examined, under authorisation, which control user permissions. Additionally, the following two RBAC standards are discussed and form part of the study's theoretical foundation: ANSI INCITS 359-2012 and ANSI INCITS 494-2012. A number of other security models are examined including the Clark-Wilson model, which also forms part of the theoretical foundation. This is followed by a discussion of accountability, which is another important part of access control. Lastly, the concept of defence-in-depth is discussed in terms of this study. The next section discusses the first component of identification.

5.2. Identification

Identification is the process whereby an entity identifies themselves by providing an identifier such as a username (Damon & Coetzee, 2013). Identification is the first step that is taken for every request that seeks to access an object. During the process of identification, the user is claiming that they are the specific individual that is linked to an identifier. However, in order to verify the claimed identity, the entity needs to be authenticated, which is covered next under authentication.

5.3. Authentication

Once the entity has identified themselves through the process of identification, the identity needs to be verified via authentication. Authentication is defined as the process of proving whether a user is who they claim to be. This is achieved by verifying whether the provided user credentials are valid. The provided credentials fall under three categories: something you know, something you have and something you are (Gregg, 2017). The following authentication methods from each of the three categories will be covered: password and Single Sign-On (SSO) (something you know), token and smart card (something you have) and biometrics (something you are). Multi-factor authentication, which falls under more than one authentication category, is also discussed. The advantages and disadvantages of these authentication methods will also be covered and are indicated in Table 5.1. The next section begins with a discussion of authentication using passwords.

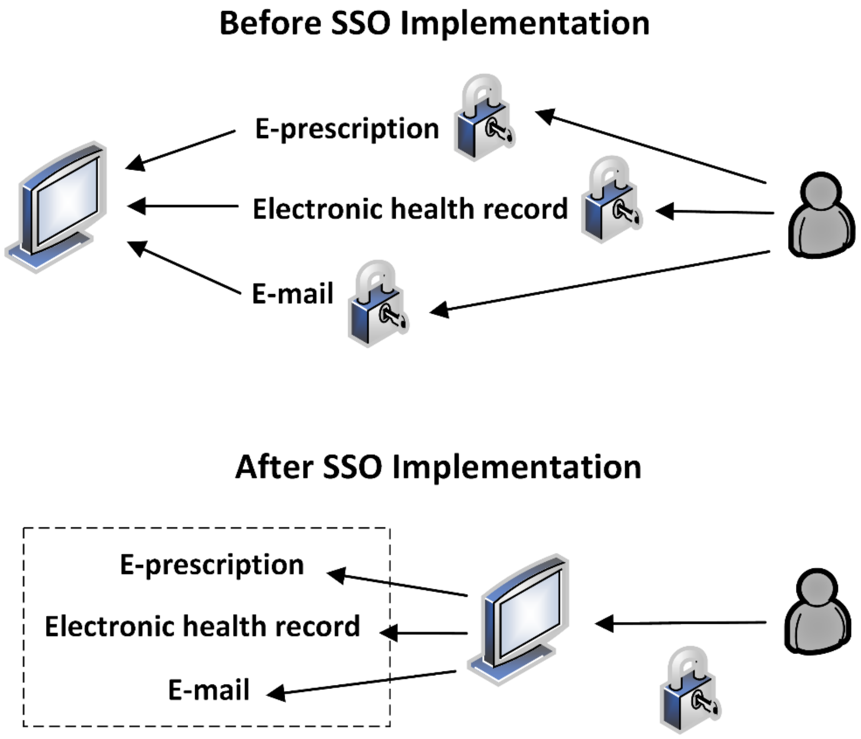
5.3.1. Password

A password is defined as a combination of characters such as letters, numbers and symbols, which should only be known by a specific user (Whitman & Mattord, 2016). A password is used in combination with a username to validate the identity of a user. A lot of emphasis has been placed on the complexity of passwords: a password should be hard to guess, thus it cannot be simple. Additionally, it should be easy to remember, but this may result in users picking a simple password. Hence, passwords that users pick may not meet the requirement of complexity. Compared to the other authentication methods from each of the three authentication categories, password-based authentication is the most common authentication method that is used (Gregg, 2017).

Passwords offer the benefit of being convenient (Brose, 2011). This is because the user (in addition to the username) only needs a password in order to authenticate. Another advantage with regards to password systems is the ease of implementation (Abu-Nimeh, 2011). However, passwords are susceptible to a number of attacks (Fernández-Alemán, Señor, Lozoya, & Toval, 2013). Password-based authentication, without sufficient cryptographic protection, is vulnerable to eavesdropping, which can result in a user's password being stolen by an attacker. Password-based authentication is also vulnerable to password cracking provided that the strength of users' passwords are weak (Whitman & Mattord, 2016). Many passwords are still vulnerable to this attack since some password systems implement weak password policies that do not enforce strong passwords. However, even those password systems that have implemented strong password policies have not resulted in the protection of passwords. Zuniga, Win, and Susilo (2010) mention that passwords may be written on sticky notes that are visible in public areas. This action could be taken by a clinician that may find it difficult to memorise a strong password. Another problem occurs when a clinician creates a supposedly strong password that complies with password policies such as 'H3@1th2018'. Although this password complies with password policies, it would still be vulnerable to password cracking since it closely resembles the weak password of 'Health2018'. Another disadvantage with passwords is that they can be shared e.g. a nurse may share their password with a co-worker who has forgotten their password (Zuniga et al., 2010). These disadvantages can place passwords at risk of being compromised. SSO, which also falls under the category of something you know, is covered next.

5.3.2. Single Sign-On

SSO is a mechanism that allows a user to log into an application once and allows the user to seamlessly access other applications without having to re-enter their credentials (Heckle & Lutters, 2011). For example, clinicians would be able to log into a number of eHealth applications, including the national EHR, once using a single set of credentials. Figure 5.1 indicates an example of a before and after implementation of SSO. Here, the clinician enters their credentials once and is able to access e-prescription, the EHR and e-mail without having to enter their credentials again. This is in contrast to the authentication architecture without SSO where the clinician would have to remember their credentials for each of the three applications. Thus, SSO addresses the problem of having to remember a large number of credentials for each application that is used. Radha and Reddy (2012) elaborates on the problem by mentioning that as the number of applications increase, the number of credentials also rise which increases the likelihood that clinicians may forget their credentials. Hence, SSO is an important mechanism that can be used to ease the process of authentication.


Before SSO Implementation

After SSO Implementation

Figure 5.1: Comparison of authentication architecture before and after SSO implementation - adapted from Heckle and Lutters (2011)

Rasiwasia (2017) mention three parties that take part in the process of SSO: the user, identity provider and service provider. The user is the entity that must be authenticated in order to access a specific service. The second party, the identity provider, is responsible for authenticating the user based on the information that is provided by the user. An identity provider also has the added responsibility of maintaining up-to-date user information. The service provider provides a service to the user by authorising them once the service provider has received and validated the authentication information of the user. The user interacts with the service provider and identity provider through an application such as a web browser. It is important to note that trust must be established between the service provider and the identity provider in order for SSO to be successful. This trust is established through a federation where an association is formed with one or more service providers and identity providers, thus enabling them to share user information with each other for the purpose of SSO.

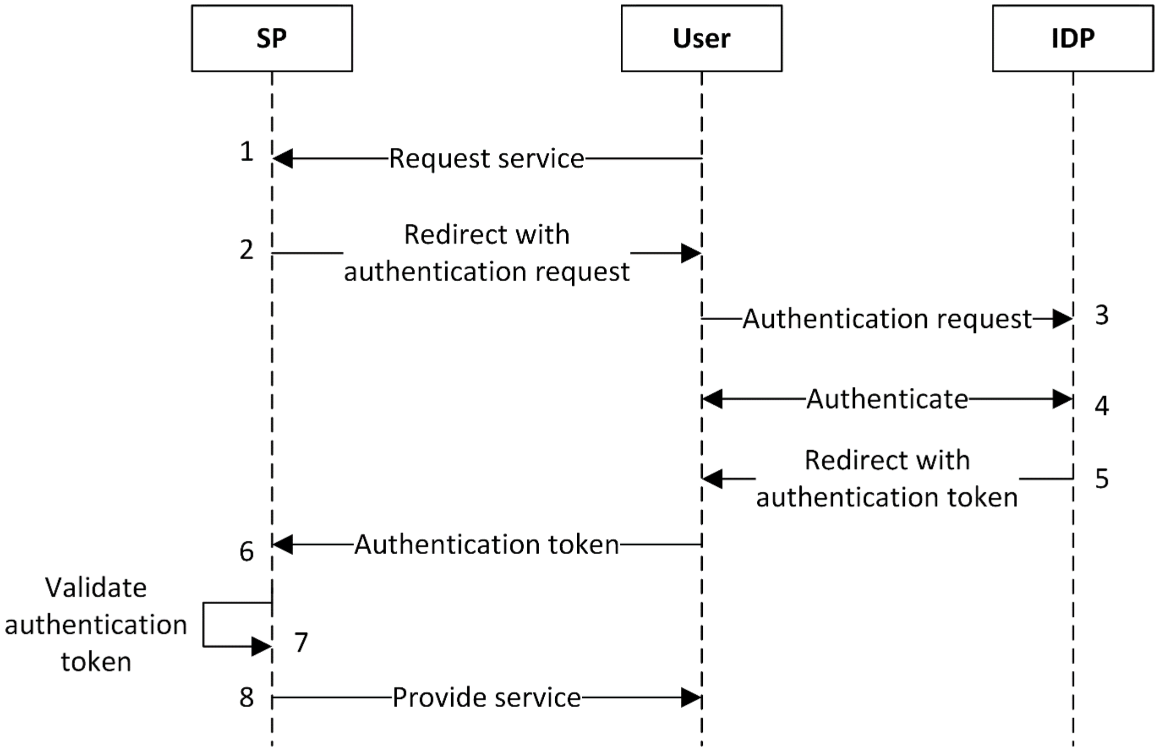


Figure 5.2: SSO workflow – adapted from Kumar (2013)

The process of authentication using SSO is discussed by Kumar (2013) as illustrated in Figure 5.2. Step 1: the user requests a service from the Service Provider (SP). Steps 2 and 3: the service provider redirects the user to the Identity Provider (IDP) with an authentication request. Step 4: the user is then prompted to authenticate with their credentials. Steps 5 and 6: once the identity provider has authenticated the user, the identity provider redirects the user back to the service provider with an authentication token, which asserts the identity of the user. Step 7:

Next, the authentication token is validated by the service provider in order to verify the identity of the user. Step 8: Once the user has been identified, they will be able to interact directly with the service provider and access the provided service. The benefit of SSO is evident when the user attempts to access another service provided by a different service provider that is also part of the same federation. In this instance, only steps 1-3 and 5-8 are repeated, skipping authentication in step 4 (Bertino & Takahashi, 2011). Thus, the user is able to access the second service without having to re-enter their credentials.

SSO can be classified into three categories: enterprise SSO, multidomain SSO and web-based SSO (Bertino & Takahashi, 2011). Enterprise SSO comprises of using the same credentials to log into multiple applications within the same enterprise, while in multidomain SSO, authentication occurs across multiple enterprises. On the other hand, web-based SSO involves using the same credentials to log into multiple web applications across the internet. In the context of this study, web-based SSO would be the most applicable type of SSO compared to enterprise and multidomain SSO. This is because web-based SSO would enable patients to access their EHR and other eHealth applications over the internet using a patient portal. The patient portal is illustrated in the proposed model in Figure 8.4.

Radha and Reddy (2012) mention a number of advantages that are provided by SSO. Firstly, SSO improves user productivity as users only have to remember a single set of credentials, thus reducing the amount of time users spend authenticating. Secondly, SSO also eases administration as only a single set of credentials need to be managed per user. However, SSO also has disadvantages as mentioned by Mustafić, Messerman, Camtepe, Schmidt, and Albayrak (2011). Using a single set of credentials results in a single point of failure. As a result, if the identity provider goes down, users will not be able to access multiple applications using SSO. Additionally, a SSO session that is left unattended by a user, who does not lock their workstation, would allow anyone to have unauthorised access to all of the user's applications. Tokens, which fall under something you have, are discussed below.

5.3.3. Token

A token is a device that is used by an authorised user to gain access to their accounts (De Soete, 2011). Unlike passwords, which is something a user knows, a token is something the user has since the user must be in possession of a token in order to authenticate. Tokens are widely used in combination with One-Time Passwords (OTPs) (Gregg, 2017). An OTP is a password that is valid for a single authentication session (Rayes, 2011). This is because once the OTP is used, it cannot be reused again in future authentication sessions. Thus, each authentication session uses a different OTP. An OTP enhances existing usernames and passwords, i.e. password-based authentication, by functioning as an extra authentication layer which increases the level of security (Huang, Huang, Zhao, & Lai, 2013). In the event that a user's password is compromised, the OTP authentication layer would prevent the attacker from gaining access to the user's account. This type of authentication is known as two-factor authentication and is covered in Section 5.3.6. OTPs can be generated by using a hard token or a soft token (NetIQ, 2016). A hard token is a physical device that is used to generate OTPs. On the other hand, a soft token generates OTPs through the use of a software application which runs on a device.

There are advantages and disadvantages with using either the soft token or hard token. Soft tokens integrate with the devices that users already possess such as smartphones (NetIQ, 2016). However, OTPs that are generated by soft tokens are susceptible to malware if the OTPs are generated on an infected device (Nguyen, 2015). This is because the OTPs can be intercepted by malware and consequently stolen. In contrast, hard tokens are not vulnerable to malware since they cannot be accessed remotely. However, a disadvantage of hard tokens is that they are prone to battery failure (Gregg, 2017). The smart card, which can also be categorised as a token, is examined below.

5.3.4. Smart Card

A smart card is a small device that is used to identify an entity (Yüksel, Küpçü, & Özkasap, 2017). The smart card is part of the category of something a user has since a user must possess a smart card before authentication can take place. The smart card is usually used in combination with another authentication method such as a password and prevents unauthorised access in the event that the smart card is lost. Combining more than one authentication method together is discussed in more detail in Section 5.3.6. Furnell et al. (2008) discuss two types of smart cards: contact-based and contactless smart cards. Authentication using a contact-based smart card takes place by inserting the smart card into a card reader. On the other hand, a contactless smart card does not need to be inserted into a card reader. Instead, authentication occurs by bringing the contactless smart card in close proximity of a card reader.

A smart card has a number of advantages compared to other authentication methods such as password-based authentication. Due to being a physical object, a smart card is harder to breach than a password (Abu-Nimeh, 2011). This is because while a password can be compromised remotely, this is not the case with smart cards. Secondly, users can tell if their smart card gets stolen. This is in contrast to passwords where in the event that the user's password is compromised, they may not be aware of this. A user can then take appropriate action to report the theft of their smart card. With regards to smart card disadvantages, Zuniga et al. (2010) mention that smart cards deteriorate over time and are also prone to getting lost. Compared to the authentication category of something you know, the user would not be able to recover their credentials and would thus have to get a new smart card. Biometrics, which refers to something you are, is covered next.

5.3.5. Biometrics

Biometrics is an authentication method where an entity's identity is authenticated through the verification of the entity's traits (Gregg, 2017). During biometric authentication, the entity attempts to authenticate by providing a certain trait. The provided trait is compared with an electronically stored trait and if a match is found the entity is successfully authenticated. Some of the provided traits include a fingerprint, facial recognition, voice recognition, retina pattern or iris pattern. However, not all types of traits are considered to be unique. In agreement, Whitman and Mattord (2016) state that only three traits are considered to be unique: fingerprint, retina and iris. Thus, since unique identification is important for accessing the national EHR, biometric authentication should comprise of one of these three traits. Biometric authentication uses one of the better methods of securing systems (Tipton et al., 2016). This is because while other authentication methods such as passwords and smart cards may be at risk of getting lost, the risk of a user losing their traits is less.

Zuniga et al. (2010) mention a number of advantages of biometric authentication. Biometric authentication is easier to use than other authentication methods. For instance, a clinician can easily access an EHR using their fingerprint. On the other hand, a clinician using password-based authentication may have a hard time accessing an EHR due to forgetting their password. Secondly, biometric authentication can be used to identify patients in an emergency situation. For example, an unconscious patient can be identified by using an appropriate trait such as a fingerprint in order to access their EHR, thus providing better healthcare. Despite these advantages, biometric authentication has some disadvantages. The accuracy of biometric authentication may sometimes be an issue where a legitimate user is not authenticated on the first attempt (Gregg, 2017). This can result in the user only being authenticated after several attempts, which could have an effect on user acceptance. Biometric authentication can also act as a barrier to disabled users. For example, a disabled user who is unable to use their hands will not be able to use biometric readers that require the use of hands or fingers for authentication. Multi-factor authentication, which is based on a combination of the previously covered authentication methods, is discussed below.

5.3.6. Multi-Factor Authentication

It is evident from the examination of the previous authentication methods that each method has its own disadvantages, where some of these disadvantages can be exploited in order to bypass the authentication method. The strength of authentication can be increased by combining authentication methods together (Gregg, 2017). Combining more than one authentication method together is known as multi-factor authentication. For multi-factor authentication to be effective, it is important for the combined authentication methods to be picked from each of the three authentication categories: something you know, something you have and something you are. Conversely, two-factor authentication is a form of multi-factor authentication that uses two of the three authentication categories to authenticate an entity (Furnell et al., 2008). Two-factor authentication can consist of the following combinations from any two authentication categories: password and biometrics, token and password or biometrics and token. The strength of this form of multi-factor authentication will depend on the combination that is chosen (Australian Cyber Security Centre, 2017). For example, selecting the combination of fingerprint and smart card would be more effective than choosing a smart card and password since a fingerprint and smart card provide a higher level of security than a password.

The benefit of using multi-factor authentication is that it strengthens authentication by adding additional layers of security (Furnell et al., 2008). In the case of two-factor authentication consisting of a password and fingerprint, an attacker would need to pass both authentication methods before gaining access to the EHR. Thus, even if a user’s password is compromised by an attacker, the attacker would not be able to access the EHR without the user’s fingerprint. On the other hand, managing more than one authentication method can be an issue when using multi-factor authentication (Aloul, Zahidi, & El-Hajj, 2009). This is because as more authentication methods are used, there is a risk that the user may lose their credentials. Abu-Nimeh (2011) states that systems requiring a high level of security should use two or three factors for authentication. Thus, due to the sensitive nature of a national EHR system, this study will be using two-factor authentication with a combination of SSO and smart card. This is covered in the proposed model in Chapter 8: Section 8.6.5.2. Authorisation, which is the third component of the IAAA, is covered in the next section.

Table 5.1: Advantages and disadvantages of examined authentication methods

Authentication Method	Advantages	Disadvantages
Password	• Convenient • Ease of implementation	• Vulnerable to eavesdropping and password cracking • Memorisation of password required • Can be shared
Single sign-on	• Improves user productivity • Eases administration	• Single point of failure • Unattended SSO session gives access to multiple applications
Token	• Soft token: integrates with user devices • Hard token: not vulnerable to malware	• Soft token: susceptible to malware • Hard token: prone to battery failure
Smart card	• Use of physical object harder to breach • Users can tell if smart card stolen	• Deteriorates over time • Can get lost
Biometrics	• Easier to use than other authentication methods • Can identify patients in emergency	• Accuracy may sometimes be an issue • Barrier to disabled users
Multi-factor authentication	• Strengthens authentication by adding additional layers of security	• Issues with managing more than one authentication method

Compiled from: (Abu-Nimeh, 2011; Aloul et al., 2009; Brose, 2011; Fernández-Alemán et al., 2013; Furnell et al., 2008; Gregg, 2017; Mustafić et al., 2011; NetIQ, 2016; Nguyen, 2015; Radha & Reddy, 2012; Whitman & Mattord, 2016; Zuniga et al., 2010)

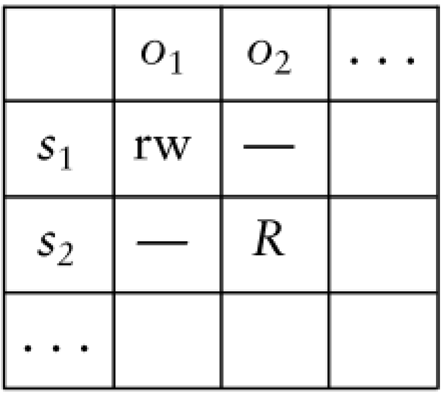
5.4. Authorisation

After a user has been successfully authenticated, the next step is to grant the user the necessary permissions in order to be able to perform certain actions on an object. This is realised through the use of authorisation, which is the process of making access control decisions in order to determine what the user can access (Rasiwasia, 2017). Authorisation is carried out using access control policies. There are a number of access control models which are based on different access control policies. In this section, four important access controls will be examined: DAC, MAC, ABAC and RBAC. Additionally, the advantages and disadvantages of each access control model will also be examined and are summarised in Table 5.3. The next section begins with a discussion of DAC.

5.4.1. Discretionary Access Control

DAC is an access control model where the owner of an object is permitted to allow or deny access to the object (Vacca, 2014). This is due to the discretionary part of DAC that enables the owner to make access control decisions with regards to the object. Furnell et al. (2008) discuss two principles that DAC is based on: 'ownership of information' and 'delegation of rights'. Ownership of information refers to the creator of an object who becomes the owner of the object. As a result, the owner has the discretion to allow or deny access to other users and can specify the type of permission e.g. read, write or execute. On the other hand, with delegation of rights a user is granted certain permissions and can pass on the same permissions to other users. While this feature could enable a patient to allow other parties to access their EHR, this could create a security risk.

Furnell et al. (2008) mention that DAC can be implemented using an access control matrix or access control list. Figure 5.3 illustrates an access control matrix which is used by most DAC systems. The rows correspond to subjects i.e. users, the columns correspond to objects while the cells correspond to permissions. An empty cell is represented by a dash that corresponds to no permissions. For example, subject S_1 has the read and write (rw) permission on object O_1, but does not have any permissions to access O_2.



	o_1	o_2	. . .
s_1	rw	—	
s_2	—	R	
. . .			

Figure 5.3: Access control matrix used by DAC (Furnell et al., 2008)

DAC provides the advantage of flexibility since the owner of an object has the authority to decide the level of permissions that are granted to another user (Alhaqbani & Fidge, 2007). This creates a second benefit that is DAC enables the sharing of objects (Mao, Li, Chen, & Jiang, 2009). However, DAC suffers from a number of disadvantages. Sifou, Hammouch, and Kartit (2017) mention that DAC allows the owner of an object to pass on permissions to other users. As a result, this puts the object at risk of being exposed to a greater amount of users. Another drawback of DAC is that it is vulnerable to Trojans (Furnell et al., 2008). The consequence of this is that the Trojan can take advantage of DAC to illegally grant permissions on objects to other users by using the identity of the owner. MAC, which makes different access control decisions compared to DAC, is discussed next.

5.4.2. Mandatory Access Control

MAC is an access control model where access is controlled based on the security level of users and objects in a system (Alhaqbani & Fidge, 2007). Unlike with DAC where access control decisions are made by the owner of the object, access control decisions are made by a central authority in MAC. MAC is based on military style security whereby users are assigned to a security clearance and objects are assigned to a security classification. The security clearance and security classification are ordered hierarchically from most secure to least secure: top secret > secret > confidential > unclassified (Furnell et al., 2008). For instance, a user who is assigned to the 'confidential' security clearance should not be allowed to read an object that is assigned to the 'secret' security classification. Additionally, a user assigned to a security clearance of 'top secret' should not be able to write to an object with the 'secret' security classification.

Table 5.2: MAC applied to a supply chain network – adapted from Chen et al. (2007)

User	Security Level	Object
Managers	Top secret	Document 1
Employees	Secret	Document 2
Individual supplier	Confidential	Document 3
All suppliers	Unclassified	Document 4

Table 5.2 shows an example of an application of MAC to a supply chain network (Chen et al., 2007). Here, each type of user is assigned to a security level (security clearance) while different types of objects such as documents would also be assigned to a security level (security classification). Managers are able to access document 1 since both the user and object are at the same security level (top secret) and can also access documents 2-4 since the managers' security level is greater than these documents. Similarly, employees can access document 2 as well as documents 3 and 4. However, employees cannot access document 1 as it is at a higher security level than the employee's security level.

The benefit of using MAC is that access control decisions are made by a central authority and not by the owner of the object as is the case with DAC (Alhaqbani & Fidge, 2007). As a result, this leads to an increased level of security since access control decisions are made by a central authority. MAC's use of a central authority for making access control decisions also allows it to defend against Trojans (Mao et al., 2009). Despite its benefits, MAC also has its disadvantages. MAC does not prevent covert channels (Alhaqbani & Fidge, 2007; Gregg, 2017). As a result, information at a high security level can be disclosed to a lower security level. MAC also does not provide fine-grained access control (Desai, 2012). Instead, users with the same security clearance are given the same permissions. Thus, each user cannot have different permissions. For example, a patient with two doctors (both assigned to the same security clearance) may not want the one doctor to view their mental illness in the EHR. However, in MAC this would not be possible as an additional security label cannot be added to the EHR to restrict the doctor from viewing this sensitive information. ABAC, which provides an alternative way of controlling access, is covered below.

5.4.3. Attribute-Based Access Control

ABAC is an access control model that uses the attributes of users and objects in order to make access control decisions (Sifou et al., 2017). It does this by comparing the user's attributes with the attributes assigned to an object in order to allow or deny access. For example, the following attributes can be used to determine if a clinician should be granted access to the EHR: location, time of day and role. A clinician that is a doctor and is located at Hospital A during their shift would be granted access to the EHR. Figure 5.4 illustrates the elements of ABAC (Furnell et al., 2008). In this model, subjects i.e. users and objects are associated with attributes that are used when deciding if access is to be granted on an object. Access is granted based on the permissions that are assigned between subject descriptors and object descriptors.

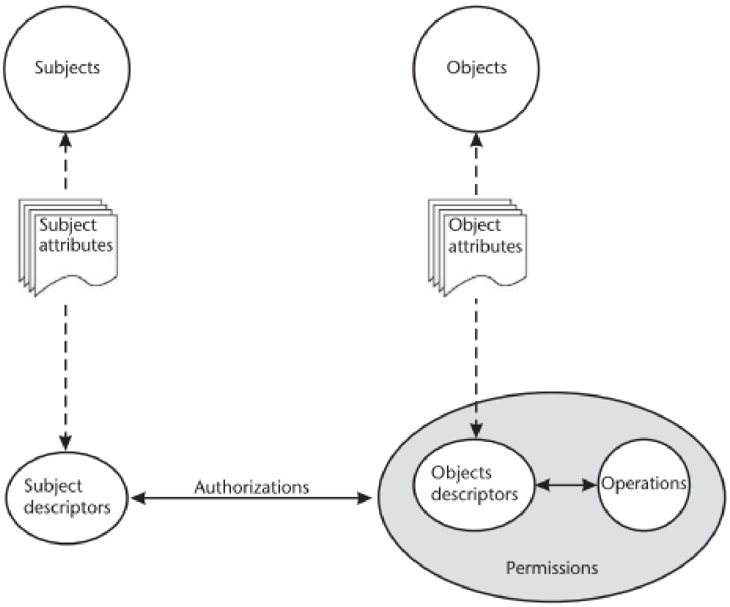


Figure 5.4: ABAC elements (Furnell et al., 2008)

ABAC provides a number of advantages over other access control models. Rasiwasia (2017) mention that ABAC provides greater flexibility. This amount of flexibility is achieved since access control decisions can be made by using a combination of various attributes. Additionally, ABAC enables dynamic authorisation. Fernández-Alemán et al. (2013) refer to this advantage as context-aware authorisation which enables access control decisions to be made using contextual information such as time of day. Despite these advantages, ABAC also has a number of downsides. In ABAC, determining the permissions of a specific user is cumbersome (Kuhn, Coyne, & Weil, 2010). Thus, management of permissions is difficult. ABAC systems that have been setup to represent the user role as an attribute also experience this disadvantage. As a result, it may be difficult to identify if a specific user has been granted excessive permissions. Another issue experienced by ABAC, as mentioned by Bertino and Takahashi (2011), is that a user's attributes may be missing or not up-to-date. As a result, an ABAC system may make an incorrect access control decision. In spite of these issues, this study will be adopting the dynamic authorisation feature provided by ABAC as this will be beneficial for controlling access to the national EHR (this is covered by the proposed model in Chapter 8: Section 8.6.5.3). RBAC, another important access control model, is discussed next.

5.4.4. Role-Based Access Control

RBAC is an access control model where roles are assigned permissions and users are assigned to these roles (Alhaqbani & Fidge, 2007). Users can perform certain actions on objects as long as their role has the necessary permissions. For example, a user that has been assigned the physician role (with read and append permissions) would be allowed to read their patient's EHR and append new information to the EHR. The manner in which access is granted using RBAC varies in comparison to the previously discussed access control models. Furnell et al. (2008) elaborates on this by stating that compared to other access control models such as DAC, RBAC eases the management of permissions through removing direct links between users and objects. In contrast, RBAC introduces an indirection through the use of roles. Hence, the use of roles is more beneficial than directly applying permissions to users as these permissions can be managed. Additionally, roles in RBAC are linked to the organisational structure of an organisation. As a result, roles defined in RBAC can follow the job functions of an organisation such as a physician, nurse and patient in the context of a hospital. The use of RBAC also enables the principle of least privilege. According to Sandhu, Coyne, Feinstein, and Youman (as cited in Helms & Williams, 2011), the principle of least privilege specifies that a user should only have the minimum set of permissions. This would ensure that a user only receives those permissions that are necessary for them to perform their job. For instance, a nurse could be given permission to only read certain parts of a patient's EHR, but under the principle of least privilege the nurse should not be given the delete permission.

RBAC provides a number of advantages. Firstly, RBAC simplifies the management of permissions through updating roles without updating individual permissions (Alhaqbani &

Fidge, 2007). This enables users to be added or removed from roles easily, while in other access control models such as DAC, permissions would need to be added or removed directly from users. Additionally, the management of permissions in RBAC gives it an advantage over ABAC in this area. Secondly, role hierarchies can be used to allow one role to inherit permissions from another role. Thus, this avoids assigning the same permissions to a new role. With regards to RBAC's drawbacks, Fernández-Alemán et al. (2013) state that RBAC does not support the handling of dynamic events and thus cannot make access control decisions when access to the EHR is being requested in the event of an emergency. Hence, RBAC does not support dynamic authorisation. However, as discussed previously, it is evident that ABAC can address this limitation that RBAC experiences. Another disadvantage of RBAC is that a specific task cannot be modelled by generic roles. For example, two physicians who have access to a certain patient's EHR would have the same permissions since they have been assigned to the generic physician role. This could result in a large number of roles being created in order to assign specific permissions such as the two roles: 'physician x' and 'physician y'.

Table 5.3: Advantages and disadvantages of examined access control models

Access control model	Advantages	Disadvantages
DAC	• Flexibility • Enables sharing of objects	• Object permissions passed on to users • Vulnerable to Trojans
MAC	• Access control decisions made by central authority • Prevents Trojans	• Does not prevent covert channels • Does not provide fine-grained access control
ABAC	• Flexibility • Dynamic authorisation	• Management of permissions difficult • User attributes may be missing or not up-to-date
RBAC	• Simplifies management of permissions • Inheritance of role permissions	• Dynamic authorisation not supported • Specific task cannot be modelled by generic roles

Compiled from: (Alhaqbani & Fidge, 2007; Bertino and Takahashi, 2011; Desai, 2012; Fernández-Alemán et al., 2013; Furnell et al., 2008; Kuhn et al., 2010; Mao et al., 2009; Rasiwasia, 2017; Sifou et al., 2017)

This study will be adopting ABAC since it provides dynamic authorisation for handling emergencies. In addition, RBAC will also be adopted since it can be applied to the healthcare context where users' job functions are based on roles. This is backed up by Fernández-Alemán et al. (2013) who state that RBAC is the most common access control model and is well-suited to health systems. The next section introduces two RBAC standards that form part of this study's theoretical foundation.

5.5. Theoretical Foundation: ANSI Role-Based Access Control Standards

The following two sections discuss two RBAC standards that serve as this study's theoretical foundation: ANSI INCITS 359-2012 and ANSI INCITS 494-2012. ANSI INCITS 359-2012 covers the RBAC standard in detail. On the other hand, ANSI INCITS 494-2012 extends INCITS 359-2012 by enabling the RBAC standard to handle dynamic events. Firstly, ANSI INCITS 359-2012 is covered below.

5.5.1. ANSI INCITS 359-2012

This RBAC standard is comprised of two main parts: the RBAC reference model and RBAC system and administrative functional specification (INCITS, 2012a). The RBAC reference model is further divided into four model components: core RBAC, hierarchical RBAC, static separation of duties relations and dynamic separation of duties relations. These four model components are depicted in Figure 5.5 and will be discussed in more detail throughout this section.

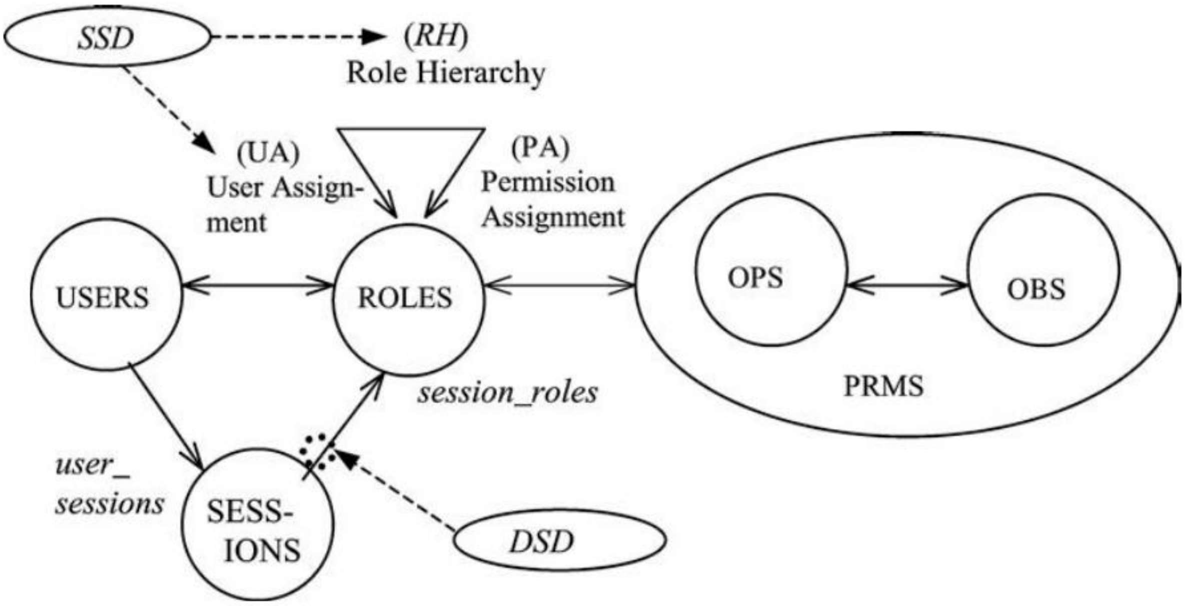


Figure 5.5: RBAC standard model – adapted from INCITS (2012a)

Core RBAC consists of five elements: users, roles, objects (OBS), operations (OPS) and permissions (PRMS). Additionally, core RBAC also includes the definition of Permission Assignment (PA) to roles and User Assignment (UA) to these roles. Also included in core RBAC are sessions. A session is defined as a mapping of a user to one or many roles. With regards to user assignment and permission assignment, Figure 5.5 illustrates arrows in both directions which indicate a many-to-many relationship. As a result, a user can be assigned to one or more roles while a role can be assigned to one or more users. Thus, as mentioned under RBAC's advantages, this eases management of permissions. In order to adhere to the RBAC standard, an RBAC system should comply with core RBAC at a minimum.

Hierarchical RBAC, the second model component, includes Role Hierarchies (RH), which are depicted in Figure 5.5. These role hierarchies are analogous to the hierarchies that structure an organisation's roles in order to represent lines of authority. Role hierarchies also specify the concept of inheritance where an inheritance relation among roles allows one role to inherit the permissions of another role. An example would be where the doctor role inherits the permissions of the employee role. Hierarchical RBAC contains two types of role hierarchies: general role hierarchies and limited role hierarchies. General role hierarchies support multiple inheritance that enables the inheritance of permissions and user memberships from two or more roles. In contrast, limited role hierarchies do not support multiple inheritance. Additionally, in limited role hierarchies, a role may have one or more direct ascendants, but is restricted to one direct descendent. Since limited role hierarchies have a simpler tree structure than general role hierarchies, limited role hierarchies were applied to the proposed model (as discussed in Chapter 8: Section 8.6.6).

The RBAC standard also covers constrained RBAC through separation of duties. Separation of duties is a control that is used to prevent users from exceeding their position's level of authority. The RBAC standard enables this through Static Separation of Duties (SSD) and Dynamic Separation of Duties (DSD). SSD implements constraints on user-role assignments in order to limit a user's permissions. This would prevent users from being simultaneously assigned to more than one role where the joint assignment of the user to these roles would violate SSD policies. For example, SSD would prevent a user from being simultaneously assigned to a role that can make changes to an EMR system and another role that can audit those changes. This is because if a user such as an administrator performs malicious operations on an EMR system, this may go undetected if they are allowed to audit these changes. In addition to applying constraints on user-role assignments, SSD is also applied to role hierarchies as shown in Figure 5.5. Consequently, role hierarchies also include inheritance of SSD constraints. Thus, inheritance of permissions and user memberships would have to comply with SSD constraints.

Similar to SSD, DSD also implements constraints to limit a user's permissions. The difference is when this constraint is implemented: SSD ensures this at the time a user is assigned to a role while DSD handles this when roles are activated in the user's session as indicated in Figure 5.5. For instance, in DSD, a user could be assigned two roles simultaneously: one that can make changes to an EMR system and another role that can conduct auditing. However, DSD would prevent the user from activating both roles simultaneously, preventing the user from auditing the changes that they made to the EMR system. The proposed model (in Chapter 8: Section 8.6.6) covers the application of DSD since the constraint on role activation provides more flexibility than SSD while still ensuring that multiple conflicting roles cannot be active concurrently.

The second part of the RBAC standard: RBAC system and administrative functional specification includes administrative commands for creating and maintaining RBAC element sets and relations such as the creation of users and user-role assignments. Secondly, it also includes administrative review functions for executing queries such as finding a set of roles that have been assigned to a user as well as what permissions have been granted to a specific role. Finally, system functions are also included for the creation and management of RBAC attributes over user sessions and for making access control decisions. This involves activating user roles within a session as well as checking if a user's activated role has the required permissions to gain access to an object. The RBAC policy-enhanced standard (ANSI INCITS 494-2012), which extends the discussed ANSI INCITS 359-2012 standard, is covered next.

5.5.2. ANSI INCITS 494-2012

While RBAC has advantages over other access control models, one of its most notable disadvantages is that it does not support the handling of dynamic events (INCITS, 2012b; Fernández-Alemán et al., 2013; Kuhn et al., 2010; Sifou et al., 2017). As a result, access control decisions made by RBAC systems cannot be further constrained by using dynamic attributes. While these dynamic attributes could be handled by an ABAC system that also uses the role attribute, RBAC's key advantage of simplifying administration would be lost (Kuhn et al., 2010). Thus, the RBAC policy-enhanced standard, which is an enhancement of the RBAC standard (ANSI INCITS 359-2012), was created to allow RBAC to handle dynamic events by

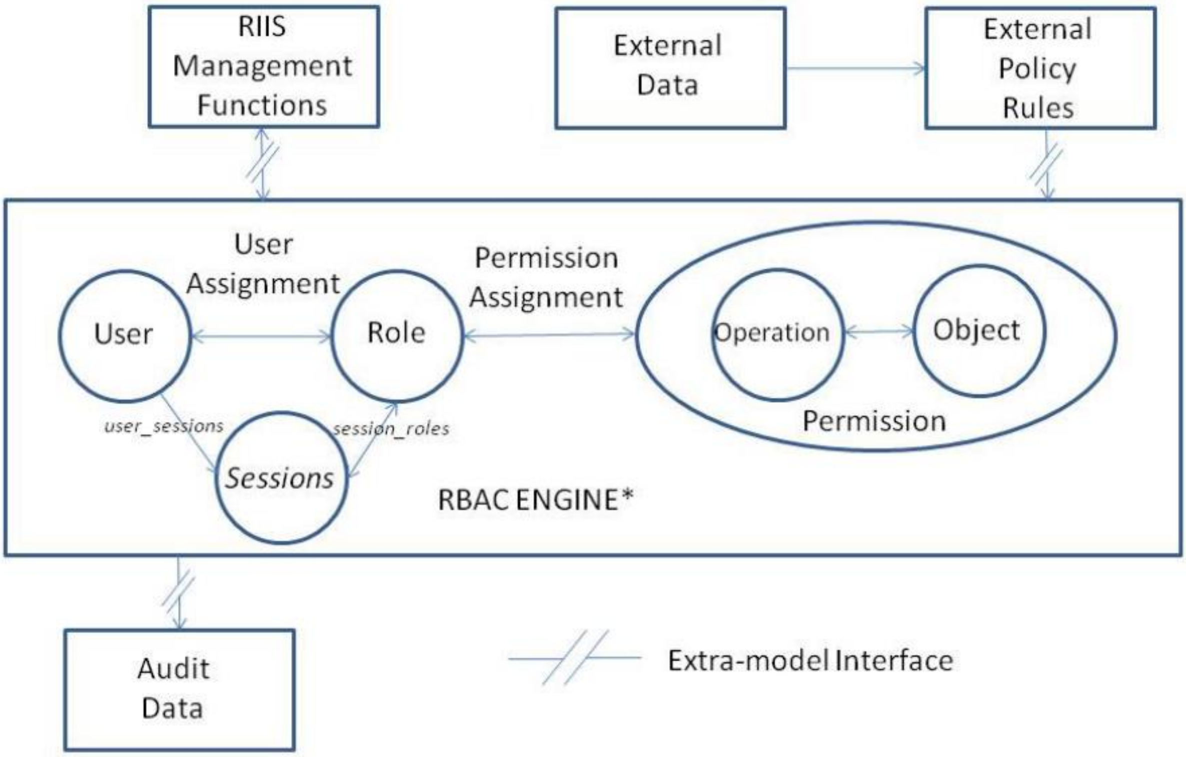


Figure 5.6: RBAC policy-enhanced reference model – adapted from INCITS (2012b)

combining the features of ABAC and RBAC (INCITS, 2012b). In addition to ANSI INCITS 359-2012, this study will also follow ANSI INCITS 494-2012 in order to use dynamic attributes with RBAC. Dynamic attributes such as location and purpose of use will allow for more flexible access control decisions. The use of dynamic attributes, in the proposed model, are discussed in more detail in Chapter 8: Section 8.6.5.3.

Figure 5.6 illustrates the RBAC policy-enhanced reference model (INCITS, 2012b). This model consists of the following components: the RBAC engine and three external interfaces (external policy interface rules, RIIS management functions interface and audit data interface). The RBAC engine contains a representation of core RBAC, which was discussed in Section 5.5.1. The RBAC engine is responsible for enforcing all access control decisions. The basis of these access control decisions are extended at runtime by introducing constraints including attributes to the RBAC engine via the external policy rules interface. As a result, access control decisions are based on both the user's role and the imported attributes. With regards to the audit data interface, the RBAC engine exports records of audit events while definitions of RBAC components are imported or exported via the RBAC Implementation and Interoperability Standard (RIIS) management functions interface. As the RBAC policy-enhanced standard is an enhancement of the RBAC standard (ANSI INCITS 359-2012), it also supports hierarchies as well as separation of duties through constrained RBAC. A number of security models, which implement some of the access control models discussed in Section 5.4, are covered next.

5.6. Other Security Models

This section discusses a number of well-known security models: Chinese wall, Bell-LaPadula, Biba and Clark-Wilson models. Additionally, the theoretical foundation of this study is also based on the Clark-Wilson model, which has a number of concepts that are applicable to a national EHR system. These security models serve as an application of the access control models that were discussed in Section 5.4. The examined security models are summarised in Table 5.4. Firstly, the Chinese wall model is examined below.

5.6.1. Chinese Wall Model

The Chinese wall model is a security model that was created to prevent conflict of interest problems (Gregg, 2017). It averts these problems by preventing an employee consulting for one organisation from accessing the information belonging to other organisations. The Chinese wall model focuses on the confidentiality of information within a commercial environment (Cankaya, 2011b). This is because conflict of interest problems exist in this context.

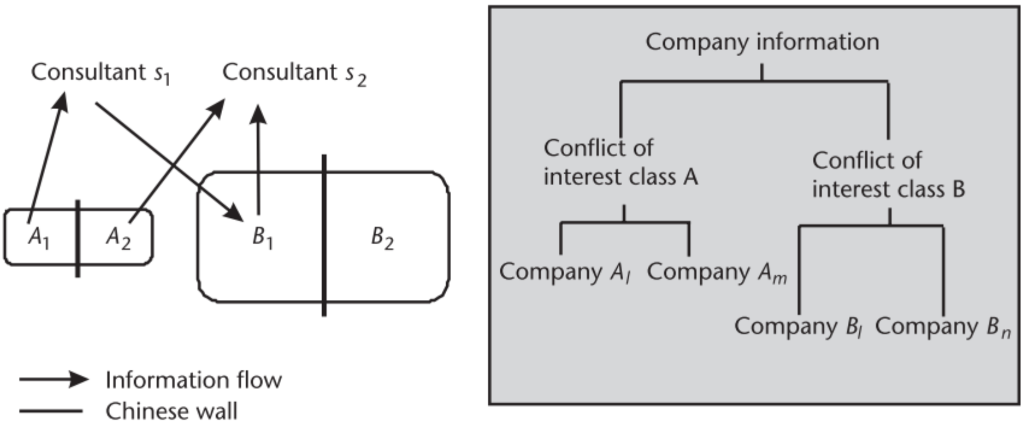


Figure 5.7: Chinese wall model – adapted from Furnell et al. (2008)

The goal of the Chinese wall model is illustrated in Figure 5.7 (Furnell et al., 2008). Here, there are two conflict-of-interest classes: A and B (A_1 and A_2 are banks while B_1 and B_2 are insurance companies). Consultant S_1 has consulted with bank A_1 and is not allowed to consult with bank A_2. On the other hand, consultant S_1 may consult with insurance company B_1 since the information flow from A_1 to B_1 would not create a conflict of interest. Although the Chinese wall model utilises features from both DAC and MAC, its ultimate goal of preventing conflict of interest problems is not applicable to this study. While the Chinese wall model may be applied to health insurance and medical aid companies, these two companies are not included in the scope of this study. Next, the Bell-LaPadula model is discussed.

5.6.2. Bell-LaPadula Model

The Bell-LaPadula model is a security model that classifies users by using a security clearance and classifies objects by using a security classification (Chen et al., 2007). Similar to the Chinese wall model, the Bell-LaPadula model is also based on DAC and MAC (Cankaya, 2011a). The Bell-LaPadula model aims to ensure confidentiality by preventing users at a certain security level from reading objects that have a higher security level. Alhaqbani and Fidge (2007) refer to this as 'no read up', which aims to prevent the unauthorised disclosure of information. The second property of the Bell-LaPadula model is known as 'no write down', which aims to prevent the unauthorised modification of information. Here, a user is not allowed to write to an object that has a lower security level than the user's security level. However, the user is allowed to write information to an object that is at a higher security level. This will not break the confidentiality of information since users at a higher security level are already allowed to read information at lower security levels. It is important to note that both the no read up and no write down rules allow a user to read or write to an object with the same security level as the user. Figure 5.8 represents a comparison between the Bell-LaPadula model and Biba model (discussed in Section 5.6.3) and shows read (r) and write (w) permissions for two subjects i.e. users (S_1 and S_2) on different security levels for objects (O_1-O_5) (Furnell et al., 2008). The information flows of the Bell-LaPadula model are represented by solid lines. For example, S_1 is allowed to read O_1 and O_2 but is not authorised to read O_3 (no read up). In

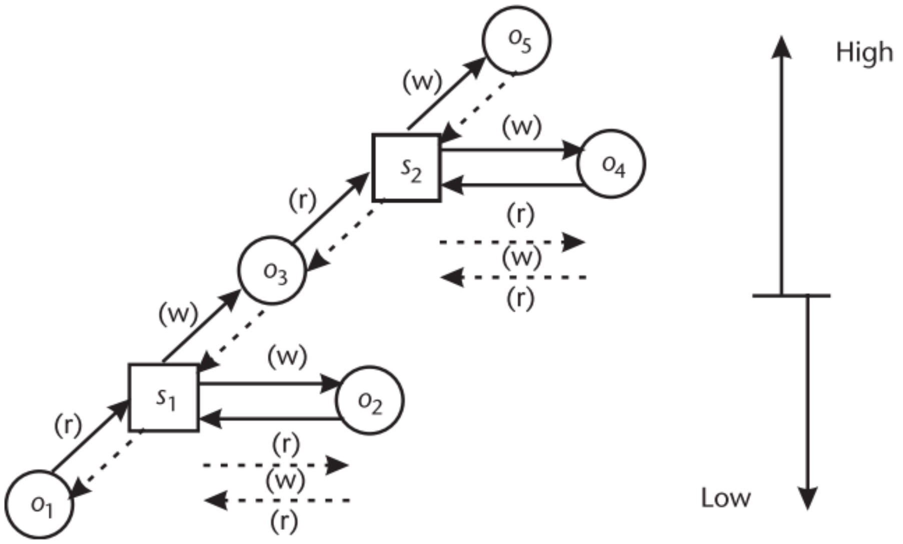


Figure 5.8: Comparison of Bell-LaPadula and Biba models (Furnell et al., 2008)

contrast, S_1 can write to O_2 and O_3 but is not allowed to write to O_1 (no write down). As the Bell-LaPadula is based on MAC, this model would not be suitable for this study due to the restriction of information flows via security levels. The Biba model, which is also based on a hierarchy of levels, is covered below.

5.6.3. Biba Model

Biba is an integrity model which states that users at lower integrity levels should be prevented from making unauthorised modifications to objects at higher integrity levels (Clark & Wilson, 1987). The Biba model is the inverse of the Bell-LaPadula model. This is evident when comparing the properties of the two models. Biba's 'no read down' property states that a user is not allowed to read an object at a lower integrity level and is the opposite of Bell-LaPadula's 'no read up' property (Estes, 2011). Additionally, Biba's 'no write up' property states that an object is not permitted to write to an object at a higher integrity level and is the reverse of Bell-LaPadula's 'no write down' property. Hence, while the Bell-LaPadula model prevents information flows from higher to lower levels, the Biba model prevents information flows from lower to higher levels that may result in unauthorised modifications of information. Figure 5.8 represents the information flows of the Biba model as dotted lines (Furnell et al., 2008). Here, S_1 can read O_2 and O_3 but cannot read O_1 (no read down). On the other hand, S_1 can write to O_1 and O_2 but cannot write to O_3 (no write up). Similar to the Bell-LaPadula model, the Biba model is also based on MAC and is thus not applicable to this study. The Clark-Wilson, which differs from the previously discussed security models, is examined next.

5.6.4. Theoretical Foundation: Clark-Wilson Model

The Clark-Wilson model is a security model that was created to ensure integrity in a commercial environment (Clark & Wilson, 1987; Gregg, 2017). However, this study will be adopting the Clark-Wilson model in the context of a national EHR (this is covered in the proposed model in Chapter 8: Section 8.6.7). This adoption is viable since the concepts of the Clark-Wilson model such as well-formed transactions, authentication, separation of duties and auditing can be applied to this new context. A well-formed transaction is a transaction where a user cannot modify data arbitrarily but can only do so in a constrained manner that would ensure system integrity (Byun et al., 2006; Schinagl, Paans, & Schoon, 2016). A well-formed transaction is only allowed to operate on verified data known as Constrained Data Items (CDIs). For instance, in order for a physician to be able to send lab results (the CDI is lab results) to a patient, they would need to do so via a specific application that has implemented integrity controls. Thus, under the Clark-Wilson model, the physician would not be allowed to directly access the data, by skipping the application, as this would result in risks to the integrity of the accessed data.

The Clark-Wilson model is also based on two other concepts that are used for enforcing well-formed transactions: Integrity Verification Procedures (IVP) and Transformation Procedures (TPs) (De Capitani di Vimercati & Samarati, 2011). IVPs verify that CDIs adhere to integrity specifications when the verification is executed. On the other hand, TPs are the only procedures that are permitted to modify CDIs (TPs correspond to the applications through which users may modify data). TPs can also take arbitrary user input i.e. Unconstrained Data Items (UDIs) and transform them into CDIs. For example, new data (UDI) that a physician enters into a patient's EHR is not covered by an integrity policy. Thus, the TP would need to validate and transform the new data into a CDI before it can be added to the system. Additionally, the results of executing TPs must meet the requirements of IVPs, which would ensure the integrity of the system.

Furnell et al. (2008) state that the Clark-Wilson model is based on roles. Users are assigned to roles that are based on their job function. The user's role is mapped to a set of well-formed transactions. The type of well-formed transactions that are assigned to the user will depend on their role. This contrasts the previously discussed security models (Chinese wall, Bell-LaPadula and Biba models) that are not based on roles. As the Clark-Wilson model is based on roles, this model includes concepts that are similar to RBAC. Another concept that the Clark-Wilson model has in common with the ANSI INCITS 359-2012 standard is the principle of separation duties (which was discussed in Section 5.5.1). In the Clark-Wilson model, separation of duties is implemented by splitting operations into subparts so that each subpart is executed by a different user, which would prevent a single user from violating the integrity of the system (De Capitani di Vimercati & Samarati, 2011). As a result, system integrity is ensured since no single user is allowed to perform an operation that would exceed their authorisation level.

The Clark-Wilson model also covers two other concepts that ensure system integrity: authentication and auditing (Clark & Wilson, 1987). In authentication, the identity of a user must be authenticated before they can execute a TP. Authentication is required in order to identify the user that has made any changes to the system. Changes made by this user via the execution of TPs must be logged in order to provide an audit trail for auditing. In this model, logs are represented as a CDI that can only be appended to.

Figure 5.9 illustrates the Clark-Wilson model. In this model, users can only modify data (CDI) via the intermediary application (TP). Also illustrated is how the TP takes CDIs (with a valid state) as input and returns new CDIs in the same valid state as before, thus ensuring system integrity. The Clark-Wilson model represents nine integrity rules for enforcing system integrity (De Capitani di Vimercati & Samarati, 2011). These rules are divided into two types of integrity rules: enforcement (E) and certification (C). Enforcement rules are enforced by the system while certification rules are executed by the administrator. An example of an enforcement rule is E2 which states that users can only access CDIs via TPs that they have been authorised to use e.g. a physician can only access a patient's EHR (CDI) via the EHR application (TP). Another example regarding a certification rule is C3 which mentions that TPs assigned to a user must comply with the principle of separation of duties e.g. the TPs assigned to an administrator should not allow the administrator to make changes to an EMR system and audit those changes. Accountability, which is the final component of the IAAA, is discussed next.

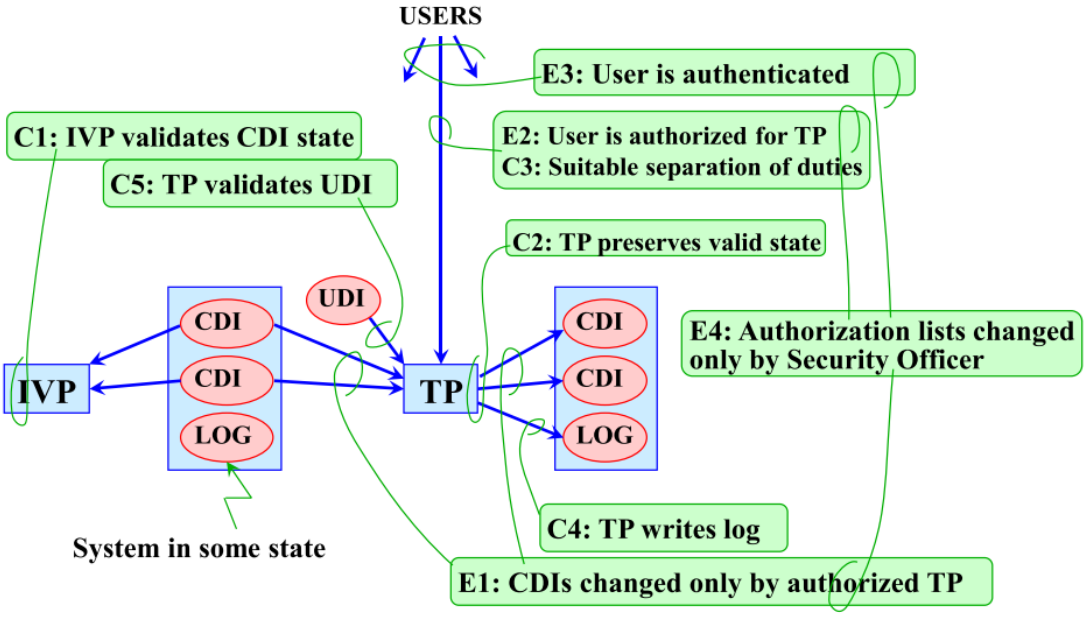

USERS
E3: User is authenticated
C1: IVP validates CDI state
C5: TP validates UDI
E2: User is authorized for TP
C3: Suitable separation of duties
C2: TP preserves valid state
UDI
CDI
CDI
LOG
IVP
TP
CDI
CDI
LOG
E4: Authorization lists changed only by Security Officer
C4: TP writes log
System in some state
E1: CDIs changed only by authorized TP

Figure 5.9: Clark-Wilson model (Schinagl et al., 2016)

Table 5.4: Summary of examined security models

Security Model	Goal	Access Control Model
Chinese wall	Confidentiality	DAC, MAC
Bell-LaPadula	Confidentiality	DAC, MAC
Biba	Integrity	MAC
Clark-Wilson	Integrity	RBAC*

Compiled from: (Dallons, Massonet, Molderez, Ponsard, & Arenas, 2007; Cankaya, 2011a; Chen et al., 2007; Furnell et al., 2008; Gregg, 2017)

5.7. Accountability

Accountability, which is also known as auditing, is an essential part of access control as it ensures that users are held responsible for their actions by tracing actions performed on a system to a user (Gregg, 2017). In the absence of auditing, the security and privacy of patients' information cannot be ensured through the use of security controls that only limit access to information (Wickramage, Sahama, & Fidge, 2016). For example, without auditing, any misuses of patient information by an authorised clinician would go undetected. Thus, in addition to security controls that limit access to information, auditing should be implemented in order to detect any misuses of patient information. The different types of auditing and monitoring for EHRs are covered below.

5.7.1. Types of Auditing and Monitoring for Electronic Health Records

Patient information has been acknowledged as being the most sensitive type of personal information (Canada Health Infoway, 2006a; Tipton et al., 2016). This is because it contains confidential information about the patient. As a result, in order to detect and respond to data breaches of patient information, the auditing and monitoring of EHR access should be done in a holistic manner. eHealth Ontario (2017) mention three types of auditing and monitoring that can achieve this: reactive, proactive and consent-related auditing and monitoring.

Reactive auditing and monitoring is often performed in response to a data breach, although it can also be performed when a patient requests to view their audit trail. It is important that this type of auditing and monitoring is performed in order to find out what happened in the event of a data breach. It also enables patients to find out what happened in their EHR and which

* The Clark-Wilson model is similar to RBAC since it is based on roles that are mapped to well-formed transactions and includes separation of duties (Furnell et al., 2008).

clinician was responsible. As a result, this ensures accountability as the clinician can be held responsible for their actions.

Secondly, proactive auditing and monitoring should be performed in order to detect unauthorised access to a patient's EHR as well as detecting any misuses of the EHR by authorised clinicians. Due to the difficulty of auditing all access to the EHR, it is more efficient to audit using a risk-based approach. This would help to detect those types of access to the EHR that pose the greatest risks to patient information. Examples of EHR access that can be monitored using the risk-based approach include the patient's EHR being accessed outside of working hours, the EHR is accessed from an unknown location, there are frequent failed login attempts, etc.

The final type of auditing and monitoring, which is also essential in the context of healthcare, is consent-related auditing and monitoring. This would involve monitoring all access to the EHR that are the result of an emergency situation. This is where the patient was not able to provide their consent to the clinician(s) and so the patient's consent was overridden in the interests of the patient's health. An example of this EHR access in an emergency situation is discussed in Section 5.7.3. It is important that all three types of auditing and monitoring are performed together and not in isolation. The audit trail, which is a fundamental part of auditing, is examined next.

5.7.2. Audit Trail

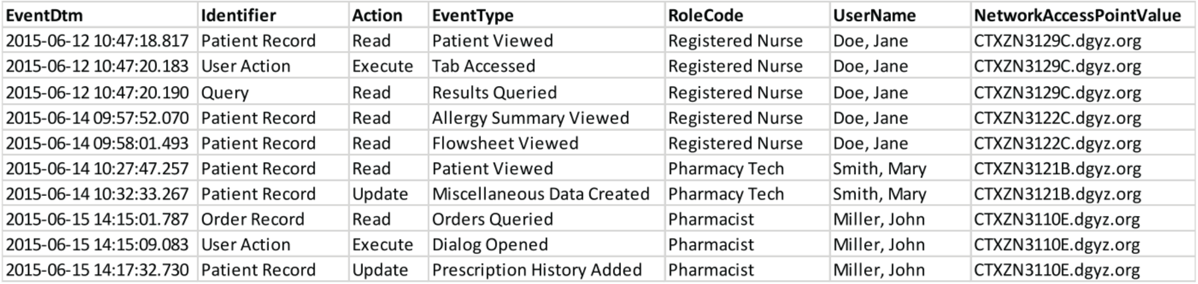
An audit trail is defined as evidence that contains the actions that were performed by entities on a system (Dekker & Etalle, 2007). The audit trail is an important part of auditing since it serves as the evidence that will be audited in order to determine whether there was any unauthorised access to the patient's EHR or if an authorised clinician misused the patient's EHR. In case of a data breach, it should be possible to find out what transpired on the affected system (Duncan & Whittington, 2016). This would provide visibility into whether the integrity of the system was modified provided that the audit trail has been recorded. In addition, since the audit trail may be the only form of evidence available, it is important that it is protected in order to prevent an attacker from tampering with the audit trail.

Chuvakin and Peterson (2010) discuss the fields that should be included in an audit trail by referring to the "Six Ws" as indicated in Table 5.5. The 'username' should be included, which will identify the clinician that accessed the EHR. Next, the 'object' field will answer what happened to the part of the EHR that was accessed while 'status' would indicate if the action

Table 5.5: Audit trail example fields (Figure 5.10) answering Six Ws – compiled from: (Chuvakin & Peterson, 2010; Sittig, 2017)

Six Ws	Field(s)	Example Field(s)
Who was involved?	username	UserName; RoleCode
What happened?	object; status	EventType
Where did it happen?	component; source	Identifier; NetworkAccessPointValue
When did it happen?	time stamp	EventDtm
Why did it happen?	reason	
How did it happen?	action	Action

conducted on the object succeeded or failed. The 'component' would determine the part of the EHR where the access occurred. Additionally, 'source' would indicate from where the access originated. The 'time stamp' is an essential field as it answers when the access occurred. The 'reason' field is also important as it indicates why the access was logged. Finally, the 'action' field will indicate the type of the event that occurred such as a login.



EventDtm	Identifier	Action	EventType	RoleCode	UserName	NetworkAccessPointValue
2015-06-12 10:47:18.817	Patient Record	Read	Patient Viewed	Registered Nurse	Doe, Jane	CTXZN3129C.dgyz.org
2015-06-12 10:47:20.183	User Action	Execute	Tab Accessed	Registered Nurse	Doe, Jane	CTXZN3129C.dgyz.org
2015-06-12 10:47:20.190	Query	Read	Results Queried	Registered Nurse	Doe, Jane	CTXZN3129C.dgyz.org
2015-06-14 09:57:52.070	Patient Record	Read	Allergy Summary Viewed	Registered Nurse	Doe, Jane	CTXZN3122C.dgyz.org
2015-06-14 09:58:01.493	Patient Record	Read	Flowsheet Viewed	Registered Nurse	Doe, Jane	CTXZN3122C.dgyz.org
2015-06-14 10:27:47.257	Patient Record	Read	Patient Viewed	Pharmacy Tech	Smith, Mary	CTXZN3121B.dgyz.org
2015-06-14 10:32:33.267	Patient Record	Update	Miscellaneous Data Created	Pharmacy Tech	Smith, Mary	CTXZN3121B.dgyz.org
2015-06-15 14:15:01.787	Order Record	Read	Orders Queried	Pharmacist	Miller, John	CTXZN3110E.dgyz.org
2015-06-15 14:15:09.083	User Action	Execute	Dialog Opened	Pharmacist	Miller, John	CTXZN3110E.dgyz.org
2015-06-15 14:17:32.730	Patient Record	Update	Prescription History Added	Pharmacist	Miller, John	CTXZN3110E.dgyz.org

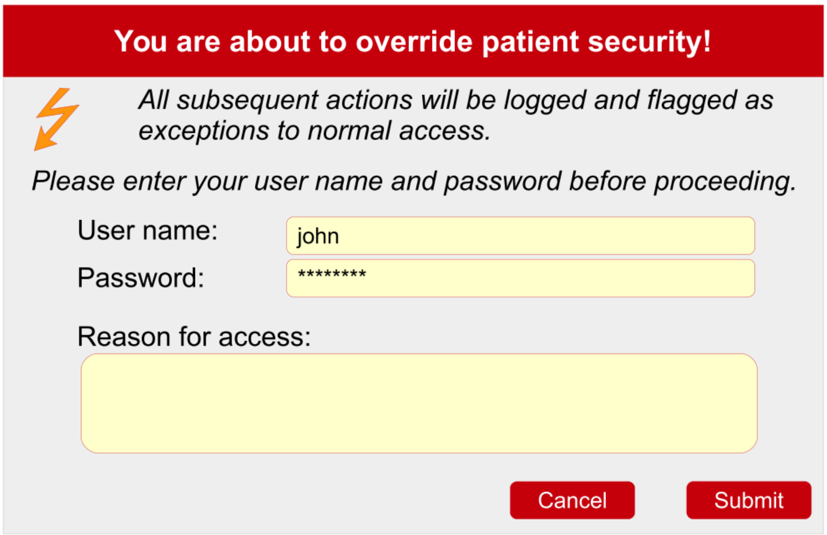
Figure 5.10: Example of an audit trail for a patient's electronic health record (Sittig, 2017)

Sittig (2017) illustrates an example of an audit trail for a certain patient's EHR (Figure 5.10). This audit trail meets five of the Six Ws that were mentioned by Chuvakin and Peterson (2010) as indicated in Table 5.5. By examining this audit trail, it can be seen that there were three clinicians that accessed the patient's EHR over a period of three days. Jane Doe (nurse) viewed the patient's EHR while also querying the patient's results. Mary Smith (pharmacy tech) viewed the patient's EHR and also updated some miscellaneous data in the EHR. John Miller (pharmacist) updated the patient's prescription history.

The use of an audit trail is beneficial since it can be used to hold a clinician accountable for the actions that they performed on a patient's EHR (Dekker & Etalle, 2007). Thus, this can deter any misuses of a patient's EHR as the clinician would be aware that their actions are being recorded in the audit trail. Another benefit is that audit trails can be used to reconstruct the events that occurred on a system (Duncan and Whittington, 2016). This can be used to investigate what happened to a patient's EHR. On the other hand, the audit trail has a number of limitations that are mentioned by Sittig (2017). Clinician A may share their credentials with Clinician B. As a result, the audit trail would not be useful since all the actions that are performed by Clinician B would be recorded in the audit trail as originating from clinician A when this is not the case. Secondly, the audit trail has a low granularity where it only indicates which screen was opened by a user but not which fields were read or modified. For example, the audit trail in Figure 5.10 does not indicate what part of the patient's EHR was viewed by Jane Doe or what information John Miller changed when updating the prescription history. Emergency access to the EHR, which should also be logged to an audit trail, is discussed below.

5.7.3. Logging Electronic Health Record Access in an Emergency

As discussed in the previous section, the audit trail serves as evidence for both authorised and unauthorised access. However, it is also important for recording the actions that are performed on a patient's EHR during an emergency. In an emergency, access control policies need to be overridden (Fernández-Alemán et al., 2013). In terms of regulations, as mentioned in Chapter 4, this exceptional access would not violate regulations as it is in the interest of the patient's health. While this is a justified reason, this type of exceptional access is a risk if not handled correctly. Exceptional access can be handled correctly while at the same time providing emergency access to a patient's EHR through the use of break-glass. Preuveneers and Joosen (2014) state that break-glass is a method of allowing a clinician, who does not have the required permissions, to access a patient's EHR in the event of an emergency. Through the use of break-glass, emergency access can be traced back to the authenticated clinician and can thus be audited. Additionally, this emergency access is temporary, hence a clinician would not retain these additional permissions after the emergency. Figure 5.11 illustrates an implementation of break-glass where the user is shown a message warning them that they do not have the required permissions to access the necessary information. The user is requested to enter their username and password before proceeding. However, this may act as a barrier to emergency access in the event that the user forgets their password. The user is also required to give a reason as to why they require emergency access. The user is alerted to the fact that their actions will be audited. Thus, break-glass can be used to provide emergency access to the EHR while at the same time being auditable. The proposed model's use of break-glass for providing access to the patient's EHR in an emergency is discussed in Chapter 8: Section 8.6.5.3. The use of auditing in defence-in-depth is covered next.



You are about to override patient security!

All subsequent actions will be logged and flagged as exceptions to normal access.

Please enter your user name and password before proceeding.

User name: john

Password: ********

Reason for access:

Figure 5.11: An example of a break-glass security warning (Preuveneers & Joosen, 2014)

5.8. Defence-in-Depth

Up until now, a number of security controls have been examined which can be used together in order to support the concept of defence-in-depth. Defence-in-depth is a strategy that aims to protect information through the use of multiple layers of security controls (Tsegaye & Flowerday, 2014; Whitman & Mattord, 2016). In the context of this study, access control as well as regulations and governance (which were covered in previous chapters) could be used together to support defence-in-depth. Although regulations and governance may not prevent a breach of patient information, both of these security controls can be used to help an organisation prepare to handle such an event. On the other hand, access control can be used to prevent a data breach. This can be achieved by implementing multiple authentication methods in layers via multi-factor authentication. Multi-factor authentication, which was covered in Section 5.3.6, can be used to support defence-in-depth (Gregg, 2017). For example, two-factor authentication can be used with a password and smart card. In the event that the password is compromised, the smart card would prevent the attacker from accessing the user's information.

Another example of access control supporting defence-in-depth is through the use of authorisation which would limit what an attacker can do. For instance, RBAC including separation of duties could be used to achieve this. Vacca (2014) states that an implementation of defence-in-depth should not only prevent data breaches but should also give an organisation time to detect and react to an attack. Detecting and reacting to an attack can be achieved through the use of auditing, which also supports defence-in-depth. For instance, even if authentication and authorisation are circumvented by an attacker, evidence of this attack would be logged in an audit trail. Thus, access control can support defence-in-depth through authentication, authorisation and auditing. This chapter is summarised in the next section.

5.9. Summary

This chapter covered access control including how it can be used to secure the EHR, which assisted with answering the research question. Securing the EHR is important since the realisation of a South African national EHR system would result in patients' EHRs being accessible nationally by an increasing number of parties. Access control can address the research problem by limiting EHR access to authorised clinicians. Firstly, access control was discussed with regards to the IAAA: identification, authentication, authorisation and accountability. The process of identification was discussed after which a number of authentication methods were covered: password, SSO, token, smart card, biometrics and multi-factor authentication. This was followed by a discussion of access control models that enable authorisation: DAC, MAC, ABAC and RBAC. In addition, two ANSI RBAC standards (ANSI INCITS 359-2012 and ANSI INCITS 494-2012) were covered. These ANSI RBAC standards formed part of the study's theoretical foundation since they allow access control decisions to be made based on a clinician's role as well as handling dynamic events such as an emergency. Next, a number of other security models were examined including the Chinese wall, Bell-LaPadula, Biba and Clark-Wilson models. The Clark-Wilson model also formed part of the study's theoretical foundation since its concepts such as well-formed transactions and auditing can assist with securing a national EHR system. Next, accountability, was examined and included a discussion of how the audit trail can be used as evidence for both unauthorised and authorised users as well as in an emergency. Finally, the defence-in-depth strategy was covered including a discussion of how access control can be implemented to support this strategy. In the next chapter, standards for an interoperable national EHR system are covered.

CHAPTER 6: STANDARDS FOR AN INTEROPERABLE NATIONAL ELECTRONIC HEALTH RECORD SYSTEM

6.1. Introduction

This chapter focusses on healthcare interoperability standards that are needed in order to ensure an interoperable national EHR system. Interoperability is defined as the extent to which two or more systems can exchange information and interpret the exchanged information (Kush, 2012). Interoperability is an important part of this study's research problem as a national EHR system cannot be established unless interoperability exists between its regional systems. Thus, this chapter aims to address this part of the research problem since without interoperability, access control cannot be enforced on a national EHR system. This chapter begins with a discussion of the three levels of interoperability which is followed by an examination of healthcare interoperability standards that can be used to address these three levels. The chapter also discusses the Health Service Bus (HSB), which can be used to ensure interoperability through the implementation of the discussed standards. Firstly, the levels of interoperability are discussed below.

6.2. Levels of Interoperability

As mentioned earlier on, interoperability is an important component of a national EHR system that would allow its EMR systems to exchange information while also interpreting the exchanged information. This is made possible by three levels of interoperability: foundational, syntactic and semantic interoperability (Broyles et al., 2016). Each level of interoperability

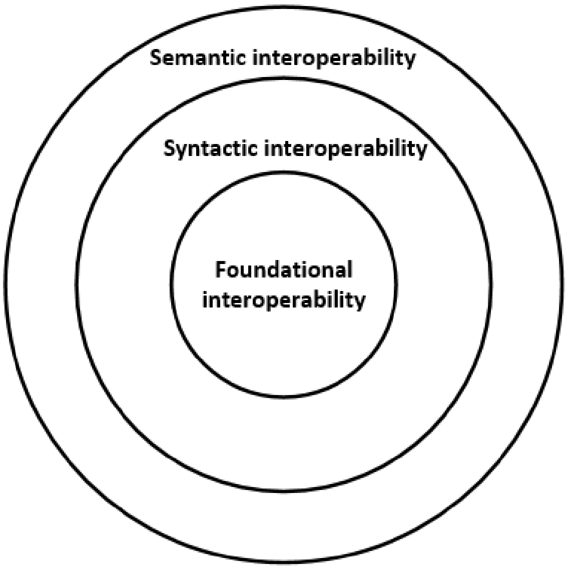

Semantic interoperability
Syntactic interoperability
Foundational interoperability

Figure 6.1: Levels of interoperability - compiled from (Broyles et al., 2016)

can be represented as a layer as illustrated in Figure 6.1. Each layer is important and together all three layers are fundamental for ensuring interoperability. This chapter focusses on healthcare interoperability standards that ensure syntactic and semantic interoperability, thus foundational interoperability standards are not covered in detail. This is because the requirements for syntactic and semantic interoperability are relatively harder to address compared to foundational interoperability (Broyles et al., 2016). Foundational interoperability, which is the first level of interoperability, is covered next.

6.2.1. Foundational Interoperability

Foundational interoperability (also known as technical interoperability) involves the transmission of information between different systems over the network (Ryan & Eklund, 2010). Thus, this level of interoperability serves as the foundation since the exchange of information between systems is the first step towards achieving interoperability. A number of communication protocols are mentioned by Frisse (2017) which systems must adhere to in order to exchange information with each other such as Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). These communication protocols specify how and where messages should be sent (Broyles et al., 2016). Thus, this would determine where a message would be delivered, which is important in the context of healthcare. For example, foundational interoperability would ensure that a patient's laboratory test results are sent to the correct doctor via the underlying network infrastructure. In the context of South Africa, many health information systems have been negatively affected by poor network connectivity as discussed in Chapter 3: Section 3.5.3. As a result, foundational interoperability cannot be realised. With regards to the scope of foundational interoperability, this level of interoperability only ensures that information is transmitted but does not indicate anything about the representation or meaning of this information (Kubicek, Cimander, & Scholl, 2011). These limitations of foundational interoperability are addressed by the other two levels of interoperability: syntactic and semantic interoperability. Syntactic interoperability, which builds on foundational interoperability, is discussed next.

6.2.2. Syntactic Interoperability

Syntactic interoperability is realised by ensuring that the messages exchanged between two systems are transmitted in a format that is recognised by both systems (Broyles et al., 2016). In order for the exchanged messages to be recognised by both communicating systems, these messages would need to be transmitted using a structure and syntax that is recognised by both systems. However, due to the large number of disparate systems in South Africa as indicated in Chapter 3: Table 3.1, realising syntactic interoperability becomes a challenge since these disparate systems do not use a common message format. In spite of this, interoperability standards are available that can address this issue and consequently ensure syntactic interoperability (these standards are discussed in Sections 6.3.1, 6.3.2 and 6.3.4). Messages that enable syntactic interoperability adhere to languages such as Extensible Markup Language (XML) which ensures that messages conform to a specific structure (Hosseini & Dixon, 2016). This specific structure is comprised of sections where each section contains a certain type of information such as a patient's first name, last name, doctor, diagnosis, etc. Syntactic interoperability is an important part of ensuring interoperability since without a specific structure, a message may not be accepted by the receiving system since its content could be represented in various ways. Hence, syntactic interoperability helps to constrain the message content by giving it a structure that would be recognised by the receiving system. Although the receiving system would recognise the message's structure, this does not ensure interoperability. This is because syntactic interoperability does not ensure that the message's content is interpreted by the receiving system (Iroju, Soriyan, Gambo, & Olaleke, 2013). Semantic interoperability, which can address this issue, is examined next.

6.2.3. Semantic Interoperability

Messages that are exchanged and are recognised as a result of foundational and syntactic interoperability are not guaranteed to be understood by the receiving system. In order for the system to interpret the received message, semantic interoperability should be present i.e. methods should exist that ensure that both the sending and receiving systems have a common understanding of certain terms (Frisse, 2017). Preserving meaning after messages have been sent from one system to another is important especially if information from disparate systems will be aggregated. For example, a national EHR would be generated by combining the information stored on disparate EMR systems. Thus, it is essential that the meaning in the content of the national EHR is preserved after the EMRs have been aggregated. Alyea, Dixon, Bowie, and Kanter (2016) discuss two methods that can be used to ensure semantic interoperability: standardisation and normalisation. Standardisation involves the use of terminology standards, which consist of a body of healthcare terms that can be used to assist with the documentation of healthcare events in a patient's EHR (these standards are discussed in Section 6.3.3). Additionally, terminology standards provide a structured and comparable language that preserves the meaning of information after it has left the sending system. This would enable two different types of systems to interpret the exchanged information as long as the same terminology standards are used by both systems. On the other hand, normalisation uses the process of mapping where the terminology used by one system is translated into another terminology that would be understood by the receiving system. Thus, it is evident that in order for semantic interoperability to be possible, both communicating systems must use a common terminology standard. In addition, it is required that standards for foundational and syntactic interoperability are implemented in order for semantic interoperability to be ensured (Kubicek et al., 2011). Standards that ensure syntactic and semantic interoperability are covered below.

6.3. Standards for Interoperability

In the previous section, the three levels of interoperability were discussed that are essential in achieving interoperability. Interoperability standards are available that address each of the three levels of interoperability. As mentioned earlier on, this chapter goes into detail with the healthcare interoperability standards that address the following two levels of interoperability: syntactic and semantic interoperability. The standards that will be discussed include the Health Level Seven (HL7) standards (HL7 v2, HL7 v3 and HL7 CDA), Digital Imaging and Communication in Medicine (DICOM) and terminology standards including Logical Observation Identifiers Names and Codes (LOINC), International Classification of Diseases - 10th Revision (ICD-10) and Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT). Additionally, Integrating the Healthcare Enterprise (IHE), which implements the previously mentioned standards, is also covered. The levels of interoperability that are addressed by the IHE initiative and healthcare interoperability standards are indicated in Table 6.2. HL7 standards for achieving both syntactic and semantic interoperability are examined next.

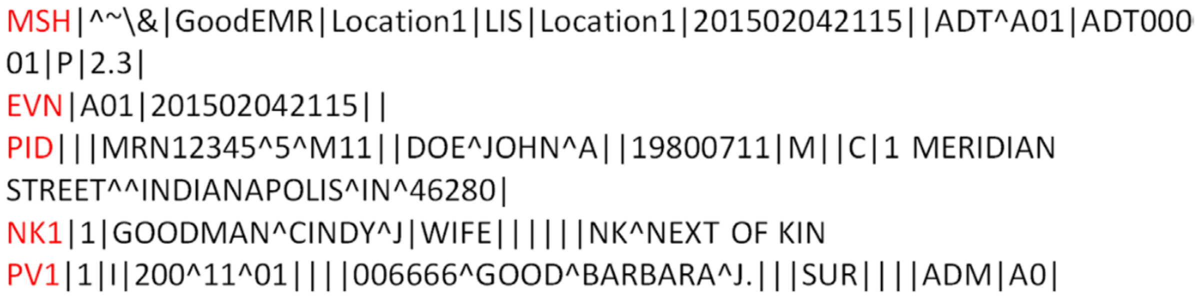
6.3.1. Health Level Seven

HL7 is an international organisation that provides standards that enable interoperability within the healthcare domain (Dolin & Alschuler, 2011). Unlike other interoperability standards that only focus on one level of interoperability, HL7 standards can be used to ensure both syntactic and semantic interoperability (as discussed in sections 6.3.1.2 and 6.3.1.3). In addition, the aim of HL7 standards is to support the electronic retrieval, sharing, exchange and integration of clinical information (Macia, 2014). This study will cover the following HL7 standards: HL7 version 2 (HL7 v2) messaging standard, HL7 version 3 (HL7 v3) messaging standard and the

HL7 Clinical Document Architecture (CDA). The HL7 v2 messaging standard is discussed below.

6.3.1.1. *HL7 Version 2*

HL7 v2 is a messaging standard that enables the exchange of clinical information between health information systems (CSIR & Department of Health, 2014). This clinical information can comprise of patient demographics, clinical observations, laboratory test results, etc. HL7 v2 is recognised as the most widely used healthcare interoperability standard in the world (Aliakbarpoor, Comai, & Pozzi, 2017; CSIR & Department of Health, 2014). HL7 messaging standards, including HL7 v2, use an event trigger model where the sending system transmits a message after a trigger has been fired (Hosseini & Dixon, 2016). The cause of the trigger is a healthcare event such as the discharge of a patient from a hospital. The receiving system can then respond to the sent message and the response will vary depending on the type of message that is received.



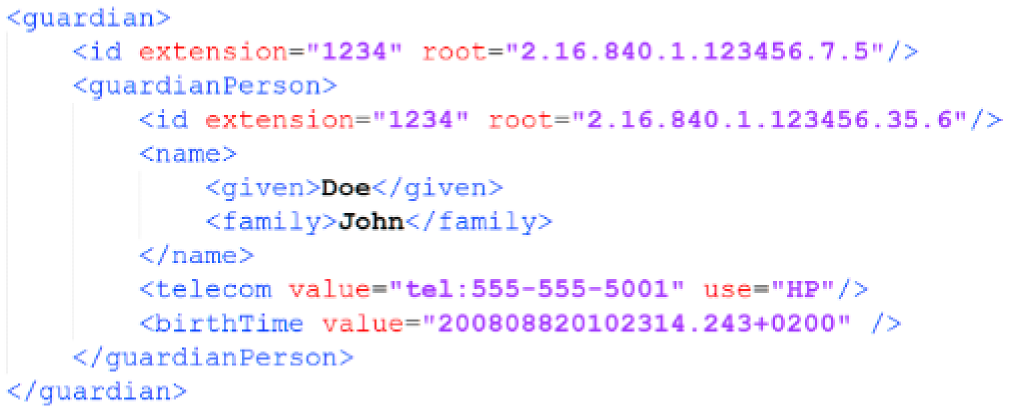
```
MSH|^~\&|GoodEMR|Location1|LIS|Location1|201502042115||ADT^A01|ADT000
01|P|2.3|
EVN|A01|201502042115||
PID|||MRN12345^5^M11||DOE^JOHN^A||19800711|M||C|1 MERIDIAN
STREET^^INDIANAPOLIS^IN^46280|
NK1|1|GOODMAN^CINDY^J|WIFE||||||NK^NEXT OF KIN
PV1|1|I|200^11^01||||006666^GOOD^BARBARA^J.|||SUR||||ADM|A0|
```

Figure 6.2: Example of a HL7 v2.3 Admission Discharge Transfer (ADT) message (Hosseini & Dixon, 2016)

Figure 6.2 depicts an example of a HL7 v2.3 Admission Discharge Transfer (ADT) message (Hosseini & Dixon, 2016). The data that is contained in a HL7 v2 message is represented by segments, fields and components. Segments are represented in red, fields are separated by the pipe (|) delimiter while the carrot (^) delimiter separates components within fields. For example, in Figure 6.2, the PID (Patient Identification) segment contains the name of the patient (John A. Doe), while ADT^A01 represents the message type, which is a patient admit message (Corepoint Health, n.d.). From this information, it is evident that John A. Doe has been admitted to a health facility. Thus, HL7 v2 ensures syntactic interoperability since a HL7 v2 message follows a certain format. The HL7 v3 messaging standard, which uses a different message format, is examined next.

6.3.1.2. *HL7 Version 3*

Similar to HL7 v2, HL7 v3 is a messaging standard that allows the exchange of clinical information between health information systems (CSIR & Department of Health, 2014). Unlike HL7 v2, HL7 v3 is based on a Reference Information Model (RIM), a fundamental part of HL7 v3, which specifies the representation of the semantics and grammar of HL7 v3 messages. Thus, through the representation of grammar, HL7 v3 ensures syntactic interoperability, while HL7 v3 also ensures semantic interoperability. Semantic interoperability is ensured since HL7 v3 messages can contain terminologies such as SNOMED CT, which is covered in Section 6.3.3.3 (Dolin & Alschuler, 2011). As a result, clinical information, which is exchanged between systems, can be represented by using terminologies that would ensure semantic interoperability.



```xml
<guardian>
    <id extension="1234" root="2.16.840.1.123456.7.5"/>
    <guardianPerson>
        <id extension="1234" root="2.16.840.1.123456.35.6"/>
        <name>
            <given>Doe</given>
            <family>John</family>
        </name>
        <telecom value="tel:555-555-5001" use="HP"/>
        <birthTime value="200808820102314.243+0200" />
    </guardianPerson>
</guardian>
```

Figure 6.3: An example section of a HL7 v3 message representing guardian information for a patient (Hosseini & Dixon, 2016)

Figure 6.3 illustrates a section of a HL7 v3 message representing guardian information for a patient (Hosseini & Dixon, 2016). Unlike HL7 v2 messages where data is structured by using pipe (‘|’) and carrot (‘^’) delimiters, the structure of a HL7 v3 message is based on XML. In the example section, tags are enclosed in ‘< >’ that contain specific data such as id, name and telephone number. Additionally, this section is structured as indicated by the indentation and colour coding inside the tags. As a result of this structured message, it can be seen that the guardian of the patient is John Doe and his telephone number is 555-555-5001. However, as stated by Hosseini and Dixon (2016), due to the complexity of HL7 v3, the majority of healthcare organisations use HL7 v2 messages instead. Despite this, the HL7 CDA standard, which is based on HL7 v3, is widely used in combination with HL7 v2 (CSIR & Department of Health, 2014). The HL7 CDA standard is discussed in more detail below.

6.3.1.3. *HL7 Clinical Document Architecture*

HL7 CDA is a standard that specifies the structure and semantics of clinical documents such as a progress note and discharge report (Heymans, McKennirey, & Phillips, 2011). This is in contrast to HL7 v2 and HL7 v3 which both focus on messages as opposed to documents. Similar to HL7 v3 messages, the structure of CDA documents is based on XML, which can be parsed by any web browser, enabling the exchange of information between disparate systems (AlJarullah & El-Masri, 2013). Thus, the CDA ensures syntactic interoperability via the use of structured documents. Additionally, since the CDA is based on HL7 v3, it achieves semantic interoperability. In agreement, CSIR and Department of Health (2014) state that the CDA is based on the HL7 RIM which supports the use of terminology standards for enhancing semantic interoperability. These terminology standards include LOINC, ICD-10 and SNOMED CT, which are discussed in Section 6.3.3. The DICOM standard, which focusses on the exchange of medical images, is examined next.

6.3.2. Digital Imaging and Communications in Medicine

DICOM is a standard that includes the storage and exchange of medical images (Pianykh, 2012). In addition to an EHR that contains patient information, the inclusion of medical images is important as medical images can provide vital information about the patient that would not be possible with text alone. Hosseini and Dixon (2016) mention how a variety of medical images, generated by different types of medical imaging devices, can be integrated by using DICOM. DICOM achieves this by integrating medical images into Picture Archiving and Communication Systems (PACS), which can exchange medical images with other systems. Thus, this facilitates the interoperability of medical images since medical images from disparate medical imaging devices can be exchanged with other systems. Terminology standards, for achieving semantic interoperability, are discussed below.

6.3.3. Terminology Standards

Terminology standards play an important role in ensuring semantic interoperability. The use of terminology standards in achieving semantic interoperability was discussed in Section 6.2.3. Terminology standards consist of a body of terms, in the area of healthcare, which are used to aid the recording of healthcare events in a patient's EHR (Alyea et al., 2016). A number of well-known terminology standards will be introduced: LOINC, ICD-10 and SNOMED CT. An example for each mentioned terminology standard will also be discussed, showing how semantic interoperability can be achieved. The LOINC terminology standard is discussed next.

6.3.3.1. *Logical Observation Identifiers Names and Codes (LOINC)*

LOINC is a terminology standard that focusses on laboratory and clinical observations (Benson, 2012). LOINC consists of codes and a name (indicated in Figure 6.4) for each concept that corresponds to a specific test result or observation measurement. Braunstein (2018) discusses an example of a LOINC name for a laboratory test. This LOINC name consists of six parts that are separated by colons. The first part indicates the substance of interest, the second part specifies the property that is measured, the third part represents the time over which the observation occurred, the fourth part indicates the type of sample, the fifth part represents the scale of the result and the sixth part specifies the method that was used to obtain the result. It is evident that this laboratory test contains medical information and meaning that would need to be preserved if it were to be transmitted to another system. As depicted with the structure of the LOINC name, a large amount of information has been represented in a compacted structure which can be interpreted by the receiving system, thus achieving semantic interoperability. Next, ICD-10, which has a different structure, is examined.

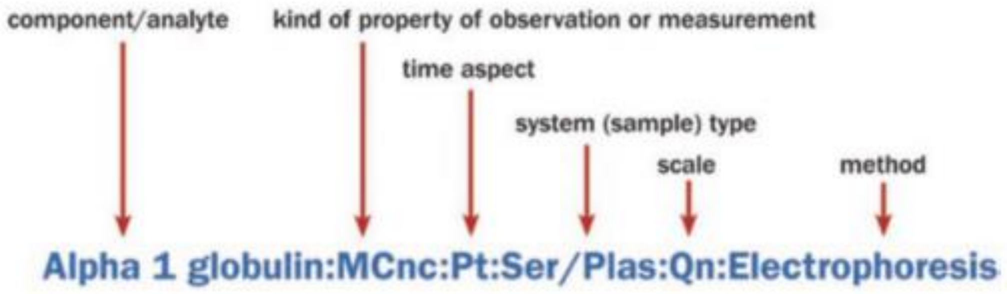

component/analyte
kind of property of observation or measurement
time aspect
system (sample) type
scale
method
Alpha 1 globulin:MCnc:Pt:Ser/Plas:Qn:Electrophoresis

Figure 6.4: Example of a LOINC name for a laboratory test (Braunstein, 2018)

6.3.3.2. *International Classification of Diseases - 10th Revision (ICD-10)*

ICD-10 is a terminology standard that covers diagnoses, health problems and conditions (Cavalini & Cook, 2015). Braunstein (2018) explains an example of an ICD-10 code for a patient with gout, as illustrated in Figure 6.5. Similar to LOINC, an ICD-10 code is also comprised of parts that provide important information about the cause, location and symptoms of the disease. The category of this health condition is chronic gout which is caused by a renal impairment. The general location of gout is in the shoulder, while the specific part of the shoulder that is affected is specified as being the left shoulder. Finally, the extension indicates that the patient is not showing the tophus symptom. By using this ICD-10 code, the following information can be recorded about the disease: the patient has gout affecting their left shoulder

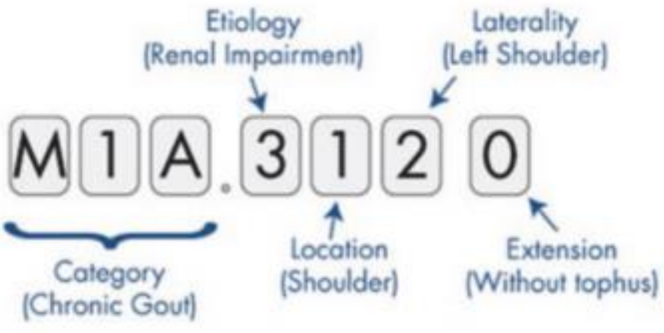


Figure 6.5: Example of an ICD-10 code for a patient with gout (Braunstein, 2018)

but has not yet developed tophus in the affected shoulder. While a computer may find it difficult to interpret the mentioned sentence, a computer would be able to parse this ICD-10 code due to its structure. Thus, the use of ICD-10 codes can ensure semantic interoperability. SNOMED CT, which can be linked to ICD-10, is covered next.

6.3.3.3. *Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT)*

SNOMED CT is a comprehensive terminology standard that represents clinical information (Benson, 2012). While LOINC and ICD-10 have a specialised focus with regards to healthcare terms, SNOMED CT includes a broad coverage of concepts representing clinical information. Braunstein (2018) discusses an example of a hierarchical view of the SNOMED CT concept, hypertensive disorder, which is associated with a nine-digit unique identifier (Figure 6.6). As illustrated, SNOMED CT indicates important clinical relationships between concepts which show the location and symptoms of this disorder. For example, the location of this disorder is the circulatory system and the symptom of this disorder is increased blood pressure. While a doctor would be able to determine that the cause of this hypertensive disorder is increased blood pressure, a computer would not be able to interpret this. Hence, through the use of a

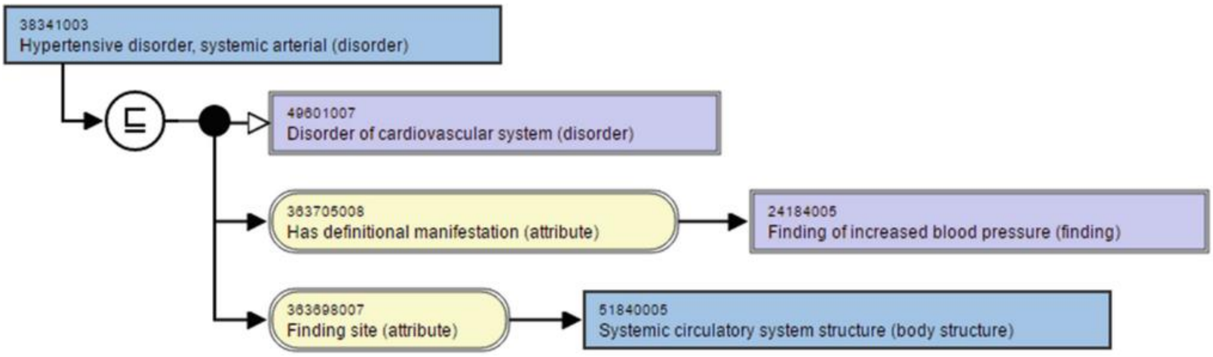

38341003
Hypertensive disorder, systemic arterial (disorder)
⊑
49601007
Disorder of cardiovascular system (disorder)
363705008
Has definitional manifestation (attribute)
24184005
Finding of increased blood pressure (finding)
363698007
Finding site (attribute)
51840005
Systemic circulatory system structure (body structure)

Figure 6.6: An illustration of the SNOMED CT hypertensive disorder (Braunstein, 2018)

clinical relationship between the hypertensive disorder and increased blood pressure, a computer would be able to interpret the cause of this disorder. As a result, semantic interoperability would be ensured.

Additionally, CSIR and Department of Health (2014) discuss an important feature of SNOMED CT that ensures semantic interoperability: mapping. This allows the terminology of SNOMED CT to be mapped to other terminology standards such as ICD-10. This would achieve semantic interoperability via a common terminology standard that would be used by both communicating systems. IHE, which implements the discussed terminology standards, is discussed below.

6.3.4. Integrating the Healthcare Enterprise

IHE is an initiative by the healthcare industry to improve the way health information systems exchange information (Macia, 2014). Hence, IHE is not a standard but instead promotes the coordinated use of well-known standards (including the discussed standards from Section 6.3) with the aim of ensuring interoperability between systems. The use of coordinated standards is essential since some standards may not be compatible with each other when used together. In agreement, CSIR and Department of Health (2014) state that some interoperability standards

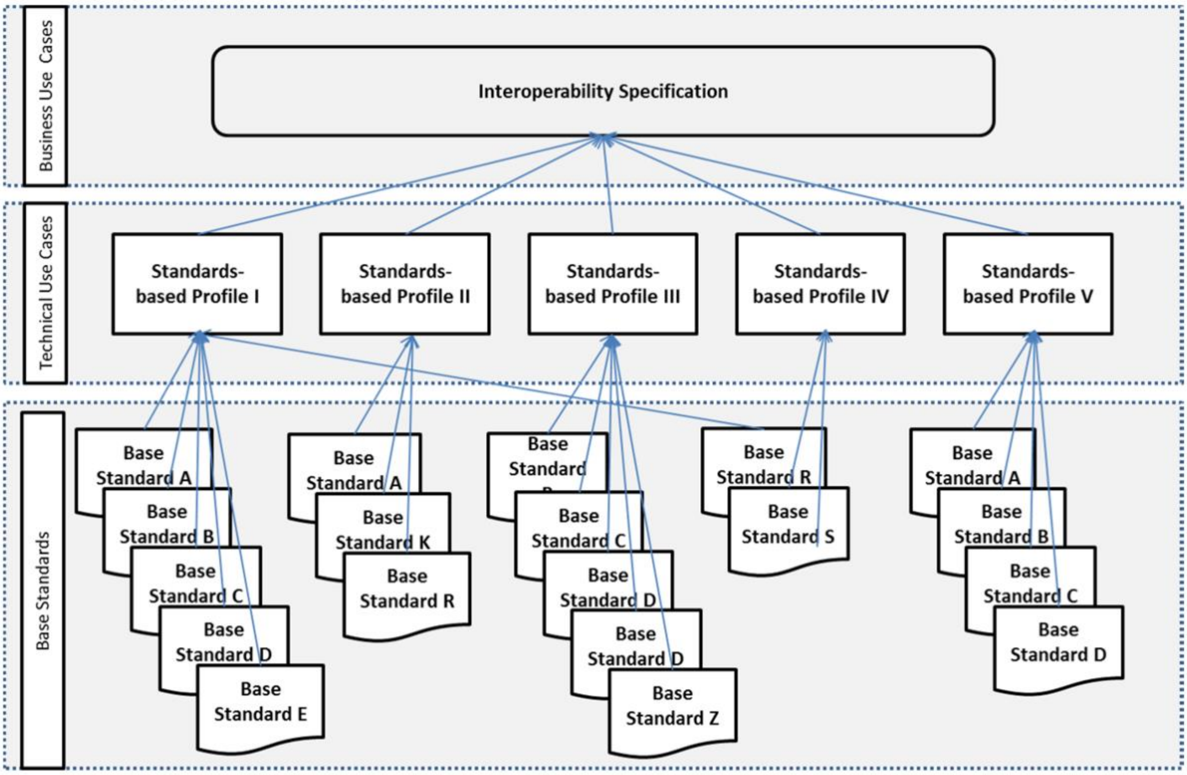


Figure 6.7: Relationship between standards-based profiles, base standards and interoperability specifications (CSIR and Department of Health, 2014)

conflict with each other. IHE addresses this issue through the use of implementation guidelines known as IHE profiles (Hosseini & Dixon, 2016). Instead of starting from the beginning by selecting a number of interoperability standards, an IHE profile specifies coordinated standards that can be implemented to ensure interoperability for a specific use case. The relationship between IHE profiles (standards-based profiles), the standards that these profiles specify (base standards) and the interoperability specifications is illustrated in Figure 6.7. CSIR and Department of Health (2014) discuss the relationship between these components, while also mentioning that base standards, standards-based profiles and interoperability specifications form the foundation for interoperability. Interoperability specifications consist of specifications that indicate how health information systems should interface with a national EHR system and should support the business use case e.g. pharmacy information system. These interoperability specifications specify the standards-based profiles e.g. IHE profiles that should be used, where each profile would address a specific technical use case e.g. 'query drug dispensed'. Finally, each profile is associated with a number of base standards that are implemented to achieve interoperability. As a result, the selection of base standards would be determined by the chosen profile, which is better than making a selection from a large number of available standards.

Table 6.1 represents a section of the National Health Normative Standards Framework, by CSIR and Department of Health (2014), for interoperability in eHealth in South Africa. This framework is aligned to this study since the specified interoperability standards are applicable in the context of a South African national EHR system. In addition, these standards are compatible with one another and can thus be used together. In this framework, functions i.e. technical use cases are mapped to IHE profiles that are in turn based on a number of interoperability standards. While the specified general IT standards assist with ensuring interoperability, this study focusses on healthcare interoperability standards, which are categorised in Table 6.1 under messaging, coding and terminology and content and structure standards (these standards were discussed in sections 6.3.1-6.3.3). In contrast with beginning by selecting these standards, an IHE profile is selected to address a specific function. For instance, the XD-LAB IHE profile would be selected to enable a doctor to query a patient's laboratory test results. In addition to the selection of general IT standards, the DICOM standard would be selected since it is required to enable the exchange of medical images, which could be contained in the laboratory test results. The HL7 v2 standard would also be selected as it is needed to enable the exchange of laboratory test results. Finally, the HL7 v3 CDA standard

Table 6.1: Mapping of functions to IHE profiles - adapted from CSIR and Department of Health (2014)

Function	IHE Profiles	General IT Standards	Messaging Standards	Coding and Terminology Standards	Content and Structure Standards
Search for patient record	PIX	XML v1.0	HL7 v2		
Retrieve and display	XDS	XML v1.0 RFC 2616 ISO/IEC 9075 ebMS ebRIM ebRS	HL7 v2		
Add, query and update clinical observations	XDS-MS	XML v1.0 RFC 2616 ISO/IEC 9075 ebMS ebRIM ebRS			HL7 v3 CDA
Add and query orders for laboratory tests	XDS	XML v1.0 RFC 2616 ISO/IEC 9075 ebMS ebRIM ebRS		ICD-10 LOINC	HL7 v3 CDA
Add and query laboratory test results	XD-LAB	XML v1.0 RFC 2616 ISO/IEC 9075 ebMS ebRIM ebRS	DICOM HL7 v2	ICD-10 LOINC	HL7 v3 CDA
Add, query and update doctor's notes	XDS	XML v1.0 RFC 2616 ISO/IEC 9075 ebMS ebRIM ebRS			HL7 v3 CDA

would be chosen since it specifies the structure and semantics (through the use of coding and terminology standards) of the exchanged laboratory test result. In addition, IHE profiles can be reused in a number of business use cases. For example, the XDS IHE profile can be used by both the pharmacy information system and laboratory information system business uses for retrieving and displaying a patient's information. The HSB, which implements standards for ensuring interoperability, is examined next.

Table 6.2: Levels of interoperability addressed by interoperability standards/initiative – compiled from (Braunstein, 2018; CSIR & Department of Health, 2014; Hosseini & Dixon, 2016)

Standard/Initiative	Syntactic Interoperability	Semantic Interoperability
HL7 v2	✓	
HL7 v3	✓	✓
HL7 CDA	✓	✓
DICOM	✓	
LOINC		✓
ICD-10		✓
SNOMED CT		✓
IHE	✓	✓

6.4. Health Service Bus

In the last section, a number of standards were covered that can be implemented to realise interoperability. These standards need to form part of a certain type of architecture in order to achieve interoperability. The Enterprise Service Bus (ESB) is a middleware software architecture with a standards-based messaging engine that is event-driven and provides important services that facilitate interoperability (Ryan & Eklund, 2010). The HSB, which is a type of ESB, achieves interoperability by enabling disparate health information systems to communicate with each other via its middleware (Hammami, Bellaaj, & Kacem, 2014). The HSB addresses all three levels of interoperability (which were discussed in Section 6.2). Foundational interoperability is ensured by connecting all the systems to the HSB (Ryan & Eklund, 2010). The realisation of syntactic and semantic interoperability by the HSB is discussed shortly.

Broyles et al. (2016) discuss the OpenHIE model, which comprises of a HSB that is represented as the interoperability layer in Figure 6.8 (the interoperability layer is hereafter referred to as the HSB). A number of systems are connected together through the HSB: Terminology Service (TS), Client Registry (CR), Shared Health Record (SHR), Health Management Information

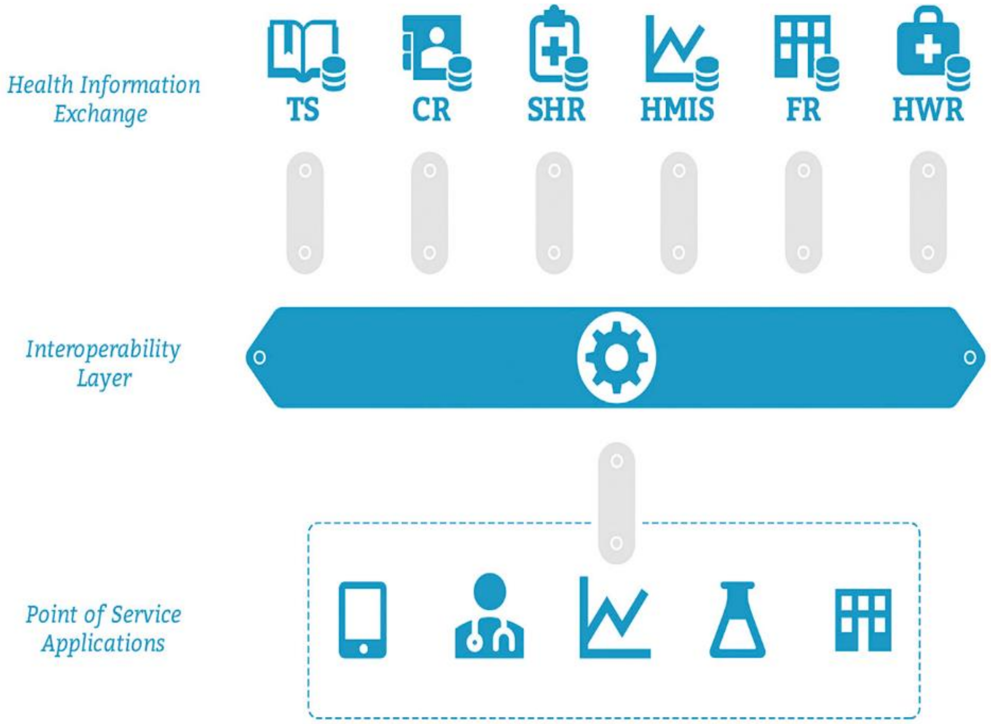


Figure 6.8: The OpenHIE model consisting of an interoperability layer i.e. health service bus (Broyles et al., 2016)

System (HMIS), Facility Registry (FR) and Health Worker Registry (HWR). Point of service applications, which are also connected to the HSB, request services from these systems. In addition, HIE, which is the electronic sharing of health information between health information systems, is illustrated and is directly supported by the HSB. Instead of implementing new systems or making major changes to existing systems, the HSB enables interoperability by interfacing existing systems through its central structure. In the event that a point of service application sends a request in a format that is not recognised by the receiving system, the HSB can transform the message into a format that is recognised by the receiving system. Additionally, the HSB will transform the response back into the format that is recognised by the point of service application that initiated the communication. Through these message transformations both syntactic and semantic interoperability can be achieved. For instance, a message in HL7 v3 format may need to be transformed into a HL7 v2 message in order to be recognised by the receiving system, thereby ensuring syntactic interoperability. With regards to ensuring semantic interoperability, the HSB calls the terminology service which maps the terminology, within the sent message, to a standardised terminology. The terminology service can then map the standardised terminology to a terminology that is understood by the receiving system. The summary of this chapter is covered next.

6.5. Summary

In this chapter, standards were covered that can enable interoperability within a national EHR system. The three levels of interoperability: foundational, syntactic and semantic interoperability were discussed. This was followed by a discussion of various healthcare interoperability standards: HL7 v2, HL7 v3, HL7 CDA, DICOM, LOINC, ICD-10 and SNOMED CT. Additionally, the IHE initiative was also covered which specifies how the discussed standards can be implemented to ensure syntactic and semantic interoperability. Finally, the HSB was examined which indicated how the discussed standards can be implemented to achieve interoperability between disparate systems. The HSB is an essential component that can assist with addressing the research problem by realising a South African national EHR system. Thus, the HSB has been included in the proposed model, which is discussed in Chapter 8: Section 8.6.9. In the next chapter, the findings and analysis of this study are discussed.

CHAPTER 7: FINDINGS AND ANALYSIS

7.1. Introduction

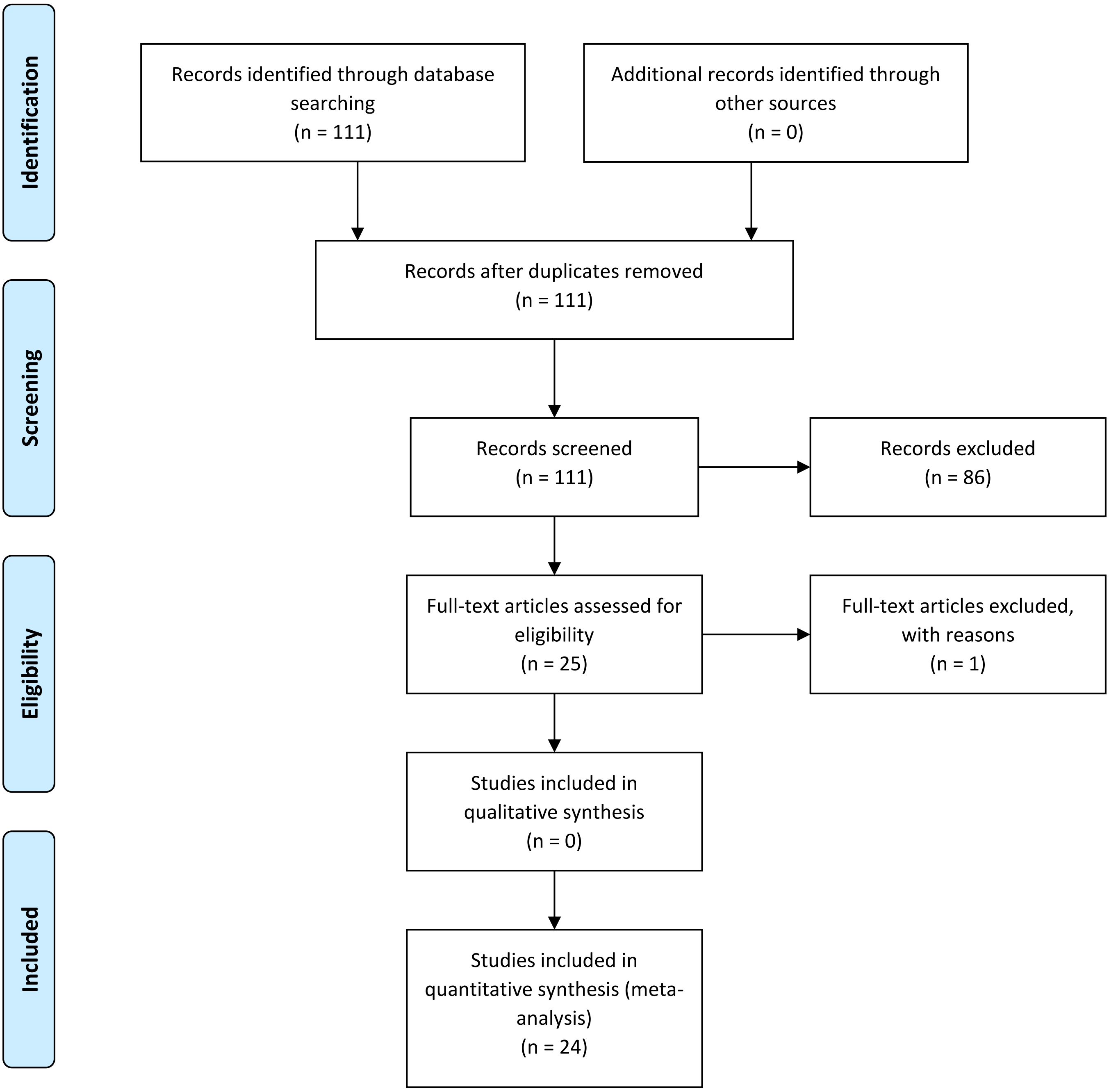
This chapter covers the findings and analysis of the content analysis and expert review, which informed the proposed model. The chapter begins by examining how the content analysis sample was selected, analysed and what the findings of the content analysis results were. Next, the results of the expert review are discussed which includes the evaluation of the proposed model and analysis of the expert review responses. Lastly, the primary observations are covered which were based on EMR and EHR implementations in the South African context. In the next section, the content analysis method, as it pertains to this study, is discussed.

7.2. Content Analysis

In this section, the results of the content analysis method are covered in detail. Content analysis consists of interpreting the meanings from textual data which results in the transformation of qualitative data into numeric data (Wahyuni, 2012). The discussion begins with how the content analysis sample was obtained using a systematic literature review which was based on the PRISMA flow diagram (Moher et al., 2009). The content analysis results are then covered which includes how the content analysis sample was coded, reduced into categories and visualised. Firstly, the selection of the content analysis sample is discussed below.

7.2.1. Selection of Content Analysis Sample

This section discusses how the content analysis sample was obtained by conducting a systematic literature review. Initially, a search query was run on the ScienceDirect database which consisted of “access control” and “electronic health record” for the years 2007 to 2017. This search was carried out in the month of May 2017. The systematic literature review was based on the PRISMA flow diagram. As a result, it consisted of four phases: identification, screening, eligibility and included as illustrated in Figure 7.1. During the identification phase, 111 peer-reviewed journal papers were returned as the results of the search query. No additional papers were identified through other sources. During the screening phase, no duplicate papers were found. Next, the screening of the 111 papers led to the exclusion of 86 papers and 25 papers remained. The method used to screen the 111 papers comprised of the following: using the previously mentioned search query on the Google Scholar database (with the addition of filtering the search results to only show papers that were published in ScienceDirect) and then selecting the first 25 journal papers appearing in both the Google Scholar and ScienceDirect databases. The use of both the Google Scholar and ScienceDirect databases for screening the papers ensured validity since the selected papers appeared in two



Identification
Screening
Eligibility
Included
Records identified through database searching (n = 111)
Additional records identified through other sources (n = 0)
Records after duplicates removed (n = 111)
Records screened (n = 111)
Records excluded (n = 86)
Full-text articles assessed for eligibility (n = 25)
Full-text articles excluded, with reasons (n = 1)
Studies included in qualitative synthesis (n = 0)
Studies included in quantitative synthesis (meta-analysis) (n = 24)

Figure 7.1: PRISMA flow diagram (Moher et al., 2009)

reputable databases. ScienceDirect was selected since most of the read literature appeared in this database while Google Scholar was chosen since it provided a filter for only retrieving ScienceDirect journal papers, which was required for the screening phase. The screening of the secondary data was initially done manually after which this process was automated by creating a script using the Python programming language, which is available in Appendix C. During the eligibility phase, 1 journal paper was excluded: *Creating a Global Rare Disease Patient Registry linked to a Rare Diseases Biorepository Database: Rare Disease - HUB (RD-HUB).* According to the title, the focus of the paper is on a rare disease patient registry while this study focuses on the EHR. After the exclusion of the previously mentioned paper, 24 papers were chosen to be used as the content analysis sample. This sample was included in the quantitative synthesis since the content analysis method was used to quantify the qualitative sample. The results of the content analysis method are covered in detail next.

7.2.2. Content Analysis Results

In this study, before the content analysis sample was coded, a test sample was imported into the MAXQDA software programme and coded in order to test whether MAXQDA was set up with the correct settings. For example, without the 'Find whole words' setting enabled (which is off by default) the coding of the term 'CIA' would match both 'CIA' and 'speCIAlised' with the coding incorrectly including the latter. This test sample was made up of three abstracts which were chosen from the original content analysis sample. These abstracts were initially created in Microsoft Word and were saved in PDF format in order to match the same format that was used by the content analysis sample. The following two codes were used for the test: 'access control' and 'security'. After these codes were applied to the test sample, the code frequencies were compared with the results of searching the test sample for the two codes using the find function. This was done to confirm whether the comparison of the code frequencies were equal. This ensured that the coding function in MAXQDA was setup correctly and that it was now ready to be used with the content analysis sample.

The 24 paper sample was imported into MAXQDA. The 24 paper sample, which was selected, represented a saturation point. While reading the papers, any terms that were related to this study were coded as they were encountered. Towards reaching the end of the sample, a saturation point was reached where the number of new codes that were added decreased substantially. This was in contrast to the coding that was done at the start of the sample, where a large amount of new codes were tagged. After all 24 papers from the sample had been read and coded, the codes were reviewed and similar codes were included. For instance, ‘authorization’ may have been coded but not ‘authorisation’ and thus should be included. Also, discretionary access control may have been coded and not its abbreviation DAC. Plural codes such as ‘EHRs’ were added since the coding of ‘EHR’ would not include ‘EHRs’ due to the ‘Find whole words’ option being enabled. Lastly, any codes with dashes were also added without dashes. For example, ‘role based access control’ was added to match some cases where a paper may have used this spelling as opposed to using ‘role-based access control’.

After the aforementioned coding was completed, this resulted in a total of 6743 tags with 228 unique codes being created. Since the number of codes was a large amount, these codes were reduced by removing duplicate codes such as ‘EHR system’ which was already included under ‘EHR’. Similar codes that were added but resulted in zero tags such as DAC were also removed. Lastly, the remaining similar codes were merged together under the same category. This resulted in some of the codes becoming categories such as ‘electronic health record’. These categories are depicted in MAXQDA as having a hierarchical structure. For example, ‘authorisation’ and ‘accountability’ are subcodes of the ‘access control’ category. Table 7.1 shows the top 30 codes before reduction. It is evident from this table that there are a number of codes that can be merged such as ‘standard’ and ‘standards’.

Table 7.2 depicts the categories after the reduction process. The codes were reduced from 228 codes to 12 codes i.e. categories. Here, the number of codes is inclusive of the category since a category is also a tagged code. The 12 codes from Table 7.2 were used to inform the proposed model. Table 7.3 represents the reduced codes with some expanded categories since some of these condensed categories are not specific. For example, the ‘standards’ category by itself does not indicate how the different types of standards were tagged in the sample. Thus, it is expanded to give insight into the various standards that were encountered, including the number of times they were tagged in descending order. Additionally, the ‘identification’ code is displayed as an independent code and is not merged with ‘access control’ in order to emphasise the IAAA which was discussed in Chapter 5.

The expansion of some categories also indicates the frequency of the subcodes according to the number of times they were tagged in the sample. As represented in Table 7.3, the ‘personal health record’ is the most tagged electronic health record, the most tagged authorisation method is ‘role-based access control’ and ‘password’ is the most tagged authentication method. Although password is the most tagged authentication method, this does not mean it is the most secure authentication method. Thus, the frequency of a code does not indicate that it is more effective compared to other codes. Other frequently tagged subcodes included 'Health Level Seven' which is the most tagged standard and 'Health Insurance Portability and Accountability Act' which is the most tagged regulation. Although HIPAA is a US regulation which is not enforced in South Africa, it was compared with other countries' regulations in Chapter 4 which included South Africa's PoPI Act. Figure 7.2 illustrates the reduced categories and some subcodes visually through the use of a hierarchical diagram. Here, the 12 categories are numbered and shaded in grey and their subcodes are shaded in white. The order of the subcodes appear in descending order from top to bottom. Lastly, Figure 7.3 represents the reduced categories and subcodes as a word cloud, with the most tagged categories/codes appearing the largest in the word cloud. The word cloud was created using the Python wordcloud library, which is available in Appendix D. The next section covers the evaluation of the proposed model via the expert review.

Table 7.1: Top 30 codes

Rank	Code	No. of tags
1	EHR	869
2	privacy	556
3	security	545
4	policy	301
5	policies	265
6	access control	262
7	standards	179
8	standard	169
9	audit	162
10	PHR	151
11	RBAC	144
12	SitBAC	138
13	electronic health record	137
14	identification	136
15	HL7	131
16	interoperability	119
17	authentication	111
18	EHRs	111
19	EHR systems	100
20	logs	94
21	authorization	90
22	EHR system	90
23	log	89
24	electronic health records	86

25	confidentiality	86
26	EMR	71
27	PCHR	68
28	XDS	64
29	HIE	63
30	IHE	60

Table 7.2: Categories after reduction

Rank	Category	No. of codes	No. of tags
1	electronic health record	23	1696
2	access control	62	1669
3	standards	35	815
4	security	5	694
5	policies	2	566
6	privacy	1	556
7	regulations	9	178
8	interoperability	1	119
9	system architecture	13	81
10	health information exchange	2	73
11	governance	1	28
12	systems theory	2	3

Note: the sum total of the subcodes in Table 7.3 do not equal the no. of tags for their parent category. For instance, the sum total of ‘personal health record’, ‘electronic medical record’ and ‘virtual electronic health records’ do not add up to 1696, since some codes such as ‘EHR' have been merged with the ‘electronic health record’ parent category.

Table 7.3: Categories expanded

Rank	Category/Code	No. of tags
1	electronic health record	1696
	personal health record	325
	electronic medical record	124
	virtual electronic health records	8
2	access control	1669
	authorisation	482
	role-based access control	193
	situation-based access control	148
	attribute-based access control	8
	discretionary access control	1
	mandatory access control	1
	accountability	423

	authentication	279
	password	50
	public key infrastructure	40
	smart card	23
	single sign-on	19
	biometrics	17
	token	14
	LDAP	4
	two-factor authentication	1
	identification	136
3	standards	815
	Health Level Seven	140
	Integrating the Healthcare Enterprise	129
	archetypes	93
	openEHR	29
	ISO 13606	22
	ISO 27799	12
	ISO 22600	9
	ENV 13729	5
	DICOM	4
	ISO 18308	4
	ISO DTS 21298	4
	CEN EN 12967	3
	ICD-10	3
	LOINC	3
	ISO 21549	2
	ISO/TR 20514	2
	ISO 10746	1
	ISO 21090	1
	SNOMED CT	1
4	security	694
5	policies	566
6	privacy	556
7	regulations	178
	Health Insurance Portability and Accountability Act	58
	Data Protection Directive	12
	Data Protection Act	3
	Personal Information Protection and Electronic Documents Act	2
8	interoperability	119
9	system architecture	81
10	health information exchange	73
11	governance	28
12	systems theory	3

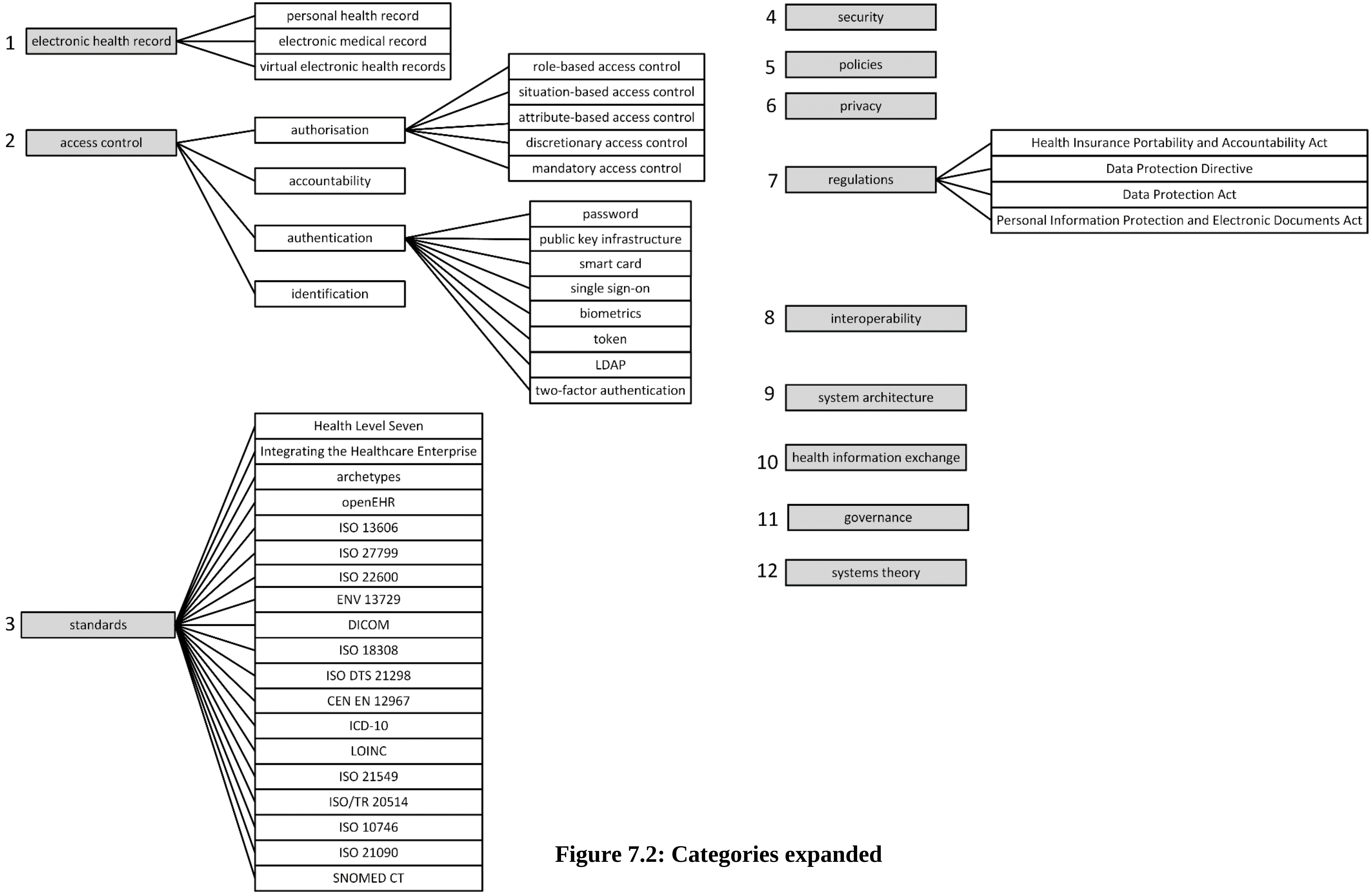


Figure 7.2: Categories expanded

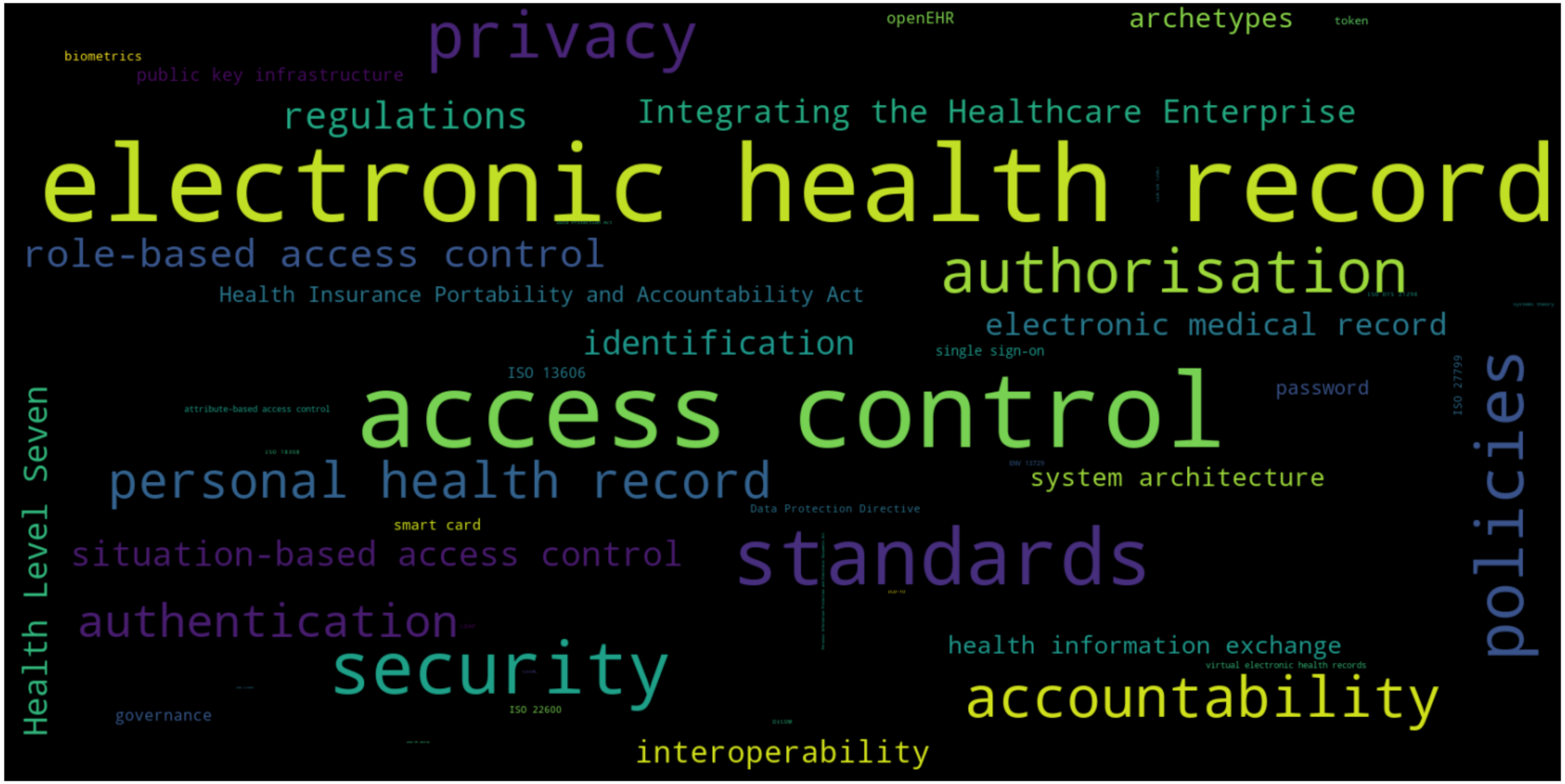


Figure 7.3: Word cloud - Categories and subcodes

7.3. Expert Review

In this section, the proposed model, which is illustrated in Figure 8.4, is evaluated using feedback which was received from the expert review. An expert review is a method for obtaining feedback from experts (Angkananon et al., 2013). The expert review responses were analysed using narration. The expert review sample comprised of ten experts: five security experts and five health experts. The five health experts consisted of three health IT experts and two medical doctors. Having experts from three different backgrounds (security, health IT and medicine) participating in the expert review allowed the proposed model to be evaluated from three perspectives. In addition, the experts in the sample originated from some of the countries that were examined in Chapter 3 including Canada, England and South Africa. The majority of the experts also have a doctoral degree which indicates that they are knowledgeable in their area of expertise. Thus, the experts were qualified to participate in the study. The questions that the experts answered are available in Appendix A. In the next section, the proposed model is evaluated using an evaluation framework.

7.3.1. Evaluation of Proposed Model

This section applies Weber's (2012) evaluation framework to the proposed model. While the evaluation framework is used to evaluate the quality of theories, it can also be used to evaluate the quality of models. The evaluation framework focuses on two perspectives: the 'parts' and the 'whole'. Using the first perspective, the evaluation focuses on the quality of its components which together make up the theory. The 'parts' comprise of constructs, associations, states and events. On the other hand, the second perspective focuses on the quality of the proposed model as a whole. The 'whole' comprises of importance, novelty, parsimony, level and falsifiability. All five criteria of the 'whole' were incorporated into the expert review questions, which were used to evaluate the proposed model.

Weber (2012) defines a construct as an attribute in general of a class of things, which is the focus of a theory. Applied to the proposed model, the things refer to the EMR systems and the class of things (or grouping) refers to a secure, private and interoperable national EHR system. Thirdly, the attributes i.e. constructs are security, privacy and interoperability (which are the focus of this study). Thus, an EMR system is considered to be part of the secure, private and interoperable national EHR system if it possesses all three attributes. With regards to associations, states and events these criteria are not applicable to the proposed model since its constructs (security, privacy and interoperability) are not quantifiable, which is required in order to be evaluated against the three mentioned criteria.

There was general consensus among the respondents that the importance of the proposed model was evident through the representation of the access control component. The importance i.e. utility of the proposed model is the manner in which its access control component controls access to the national EHR while also auditing and enabling emergency access in the interest of a patient's healthcare. Access control is important since it ensures that the patient's EHR will only be accessed by authorised clinicians and that the clinicians only have access to patient information which is required to do their job function.

With regards to novelty, the proposed model has made a contribution of improvement (as discussed in Section 8.6). A contribution can be considered novel in the following ways: the contribution frames well-known focal phenomena in new ways and the contribution makes important changes to an existing model such as adding constructs (Weber, 2012). Examining the first condition, the proposed model has framed the IAAA in the context of a national EHR system. The available access control models from the literature do not illustrate the use of the IAAA for securing the national EHR. With regards to the second condition, the proposed model has made important changes to the national EHR system architectures of the examined countries (from Chapter 3: Section 3.4.3) by illustrating how regulations inform access control. In addition, the relationship between the EMRs and how they form the EHR is illustrated. The proposed model also presents the concept of tiered EHRs by indicating how the second tier EHR and first tier EHR are generated with and without the distributed architecture respectively. Most of the respondents agreed that the contribution of the proposed model is novel.

A theory is considered to be parsimonious if it achieves a good degree of explanatory power in connection with its focal phenomena while using a small number of constructs (Weber, 2012). The majority of respondents indicated that the number of components in the proposed model were adequate. As a result, the explanation of the proposed model's focal phenomena i.e. access control is not hindered by the surrounding components.

In terms of level, some theories cover their phenomena in a broad or specific way. Most of the respondents indicated that the proposed model covered its phenomena in a broad way. Although the proposed model focuses specifically on access control, a number of other components are also included which are required in order for a national EHR to be realised (which access control will ultimately secure) such as interoperability and EMRs. As a result, the broad number of phenomena emphasise the context and manner in which access control will operate.

With regards to falsifiability, all of the respondents were in agreement that the proposed model could be tested. Although this study does not focus on the implementation of the proposed model, the implementation of a prototype based on the proposed model could be used in order test the model in the real world.

Based on the above evaluation of the proposed model, the respondents found that the proposed model focused on important phenomena, it was novel and parsimonious, the level of the proposed model was appropriate for its context and finally the proposed model was falsifiable. Expert review responses pertaining to other aspects of the proposed model are covered next.

7.3.2. Other Expert Review Responses

This section analyses other aspects of the proposed model which did not form part of the previous section's evaluation. The feedback on the proposed model was generally positive with a respondent indicating that the proposed model imposes a structure on how clinicians would access the EHR while another respondent mentioned that the relevance of the proposed model was stated in comparison to existing models.

All of the respondents were in agreement that the proposed model addressed a relevant research problem. The research problem states that there is complexity involved in balancing the requirements of security, privacy and access of the EHR. Additionally, the security and privacy of patients' EHRs are at risk due to the sharing of the EHRs with an increasing number of parties. The proposed model addresses the research problem through the use of access control which ensures the security and privacy of the patient's EHR by limiting EHR access to authorised clinicians while also ensuring that authorised clinicians only have access to parts of the EHR that they need to know.

With regards to the study's theoretical foundation, there was general consensus that the theoretical foundation is relevant for securing a national EHR system. The theoretical foundation of this study (ANSI RBAC standards and Clark-Wilson model) was applied to the proposed model in Chapter 8: Section 8.6.6 and 8.6.7. The relevance of the chosen theoretical foundation is that access to the patient's EHR is controlled based on the role of the clinician. Additionally, dynamic events such as emergencies are handled by ABAC. Also important is the application of the Clark-Wilson model which ensures the integrity of the EHR by only allowing the modification of the EHR in a constrained manner.

One respondent mentioned that the proposed two-factor authentication (smart card and SSO) may not be feasible since some clinics operate where one user logs in for a day. This would result in the clinician's account being shared with other clinicians. However, this practice is not secure as there is no accountability. As discussed in Chapter 5: Section 5.7, any malicious actions performed on the system would be attributed to the clinician who shared their account even though the clinician did not perform such an action. Two-factor authentication can address this issue while also being usable: clinicians would only need to insert a smart card into a smart card reader and enter a password once. This is the result of SSO where clinicians would not be prompted to reauthenticate when accessing other eHealth applications. Another respondent suggested the use of biometric authentication as part of two-factor authentication. Biometric authentication (fingerprint) with SSO was the study's initial choice for two-factor authentication. However, since clinicians in some health facilities perform their job functions using clinical gloves, it was decided that biometric authentication would be replaced with smart card authentication since clinicians that wear clinical gloves would be able to authenticate.

There was general consensus among the respondents with the proposed model's use of the distributed architecture for accessing the national EHR. A respondent indicated that the selection of the distributed architecture was good because it enables interoperability, real-time update of the EHR as well as operational and secure functionality. This is in agreement with the distributed architecture advantages that were discussed in Chapter 3: Section 3.4.2 such as the latest patient information being available (real-time update of the EHR) as well as increased level of security and no single point of failure (operational and secure functionality).

With regards to recommendations, a respondent suggested that the proposed model could be enhanced by producing a set of diagrams using overview and zoom that would represent different aspects of the model. This has been incorporated into the proposed model throughout Chapter 8: Section 8.6 which includes detailed diagrams of the following components: EHR, authentication, authorisation, regulations and interoperability. Based on the received feedback, no other changes were made to the proposed model other than the inclusion of the detailed diagrams. The next section discusses the primary observations of the author with regards to the implementation of the EMR/EHR in three South African health facilities.

7.4. Primary Observations

This section discusses three hospitals that implemented an EMR/EHR system, which is based on the author's observations from the public sector in South Africa. All three of these hospitals are based in the Eastern Cape province. Each hospital that is discussed is mentioned using the following format 'Eastern Cape Hospital x' where x is a number. The first observation, which is covered, discusses the EMR implementation of Eastern Cape Hospital 1.

7.4.1. Use of EMR System within Hospital

An EMR system, from a single vendor, had been implemented in Eastern Cape Hospital 1 which included modules for patient registration, laboratory, radiology as well as pharmacy. Although it was utilised in different departments such as radiology, clinicians found it cumbersome to use at times for various reasons such as the user interface which was text based. At the time of the observation, the hospital was looking for another EMR system to use. The challenge that was observed in Eastern Cape Hospital 1 was discussed in Chapter 3: Section 3.5.4. An observation of a Customer Relationship Management (CRM) system functioning as an EMR system is discussed next.

7.4.2. CRM used as EMR System within Hospital

This observation refers to Eastern Cape Hospital 2 which used a CRM system as its EMR system. The CRM system was customised with modules including patient registration, patient billing, pharmacy as well as an inpatient module. However, only the patient registration module was utilised and the other modules were not used. One of the reasons was due to a lack of training and technical support. It was also observed in the patient registration module that some of the captured information contained errors and not all fields were captured. In addition, it was observed that the clerks who entered the patient information into the patient registration module, simultaneously created a paper-based record. The challenges that were observed in Eastern Cape Hospital 2 were covered in Chapter 3: Section 3.5.1, 3.5.4 and 3.5.8. The next observation mentions the use of the same EHR system by a number of hospitals.

7.4.3. Use of EHR System within Hospitals

An in-house EHR system was implemented at Eastern Cape Hospital 3 and used throughout the hospital. It was later piloted in five other Eastern Cape hospitals. Although this EHR system is not functioning as a national EHR system, the EHR system was able to interface with the Eastern Cape hospitals that took part in the pilot and also implemented HL7 standards. Some of the modules included in the EHR system were radiology, pharmacy, laboratory and a clinician module for recording patient encounters. The findings and analysis chapter is summarised in the next section.

7.5. Summary

This chapter focussed on the findings and analysis of this study which included a discussion of the content analysis as well as how the proposed model was evaluated via an expert review. The content analysis discussion covered how a systematic literature review was conducted in order to obtain the final content analysis sample. This was followed by a discussion of the content analysis results which focussed on how the content analysis sample was coded, reduced and later visualised. Next, the expert review was covered where the proposed model was evaluated using Weber's (2012) evaluation framework with the results indicating that the proposed model met the five examined criteria. In addition, other expert review responses were analysed, through the security, health IT and medical perspectives, with the feedback on the proposed model being generally positive. Finally, the primary observations based on the EMR/EHR implementations in South African health facilities were covered, which indicated that there was an alignment with some of the discussed challenges in Chapter 3: Section 3.5. In the next chapter, the recommendations and proposed model are covered.

CHAPTER 8: RECOMMENDATIONS AND PROPOSED MODEL

8.1. Introduction

In this chapter, the proposed access control model, which is the contribution of this study, is covered in detail. Firstly, the research problem is revisited and is followed by a discussion recapping how the proposed model was developed. Critical thinking, which was central to the development of the proposed model, is also covered including the study's argument diagram which justifies the proposed model's key components. This is followed by a discussion of the proposed model in terms of its key components. The chapter also covers the application of the general systems theory to the proposed model. The next section revisits the research problem of this study.

8.2. Research Problem Revisited

As discussed in Chapter 1: Section 1.2, the research problem of this study was identified. The research problem is that there is complexity involved in balancing the requirements of security, privacy and access of the EHR. The security and privacy of patients' EHRs are at risk due to the sharing of the EHRs with an increasing number of parties. This complexity would need to be addressed through the use of access control, which is covered by the proposed model in Section 8.6.4. Additionally, access control and interoperability are linked: without interoperability, access control cannot be enforced on a national EHR system as this system would not exist without interoperability. Thus, the proposed model also indicates how interoperability can be realised in a national EHR system. The development of the proposed model is discussed in the next section.

8.3. Development of Proposed Model

The development of the proposed model was the result of a number of research methods that were conducted in this study. The initial creation of the proposed model was informed by the results of the content analysis method. The content analysis method was conducted using the MAXQDA software programme on a literature sample in the area of access control and the EHR. The literature sample was read and key terms were tagged as codes. These codes were reduced to 12 codes which were used to inform the proposed model (the results of the content analysis method were covered in Chapter 7: Section 7.2.2). The proposed model was also informed by conducting an extensive literature review using critical thought on Chapters 3-6. Relevant concepts originating from each of these chapters were incorporated into the proposed model in the form of components, which assisted in addressing the research problem. The proposed model was further refined using the expert review method (as discussed in Chapter 7: Section 7.3), which was also used to evaluate the credibility of the proposed model. The expert review consisted of both security experts and health experts which ensured that the proposed model was analysed from more than one perspective. Central to the development of the proposed model was the use of critical thinking, which was used throughout the study. Critical thinking is defined as the skill of critically evaluating the arguments of others while creating your own good arguments (Rainbolt & Dwyer, 2012). The inclusion of key components in the proposed model was justified by using critical thinking which resulted in an argument diagram (as discussed in Section 8.5). The next section covers critical thinking in more detail.

8.4. Critical Thinking

As discussed earlier on, critical thinking involves critically evaluating the arguments of others while also creating good arguments of your own. An argument provides reasons which support a belief (Rainbolt & Dwyer, 2012). As illustrated in Figure 8.1, every argument should consist of two parts: premises (the reasons) and the conclusion (the belief that is supported by the reasons). Thus, the premises serve as the reasons that support the conclusion.

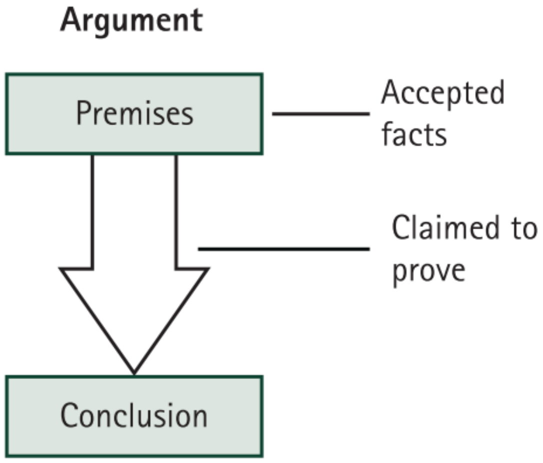


Figure 8.1: Illustration of the two parts of an argument (Rainbolt & Dwyer, 2012)

Premises and conclusions can also be represented in an argument diagram which indicates how they are linked together. This is depicted in Figure 8.2 where each statement (both premises and conclusions are statements) is represented by a number in a circle (Rainbolt & Dwyer, 2012). Here, statements that function as premises have an arrow pointing away from them while statements functioning as conclusions have an arrow pointing towards them. It is also possible for the conclusion of one argument to serve as the premise i.e. sub-conclusion of another argument (Walker, 2011). For instance, Figure 8.2 indicates that the first statement (premise) supports the second statement (sub-conclusion) which in turn supports the fourth statement (conclusion). Additionally, the third statement also supports the fourth statement. In the next section, the argument diagram of this study is presented which justifies the key components that form part of the proposed model.

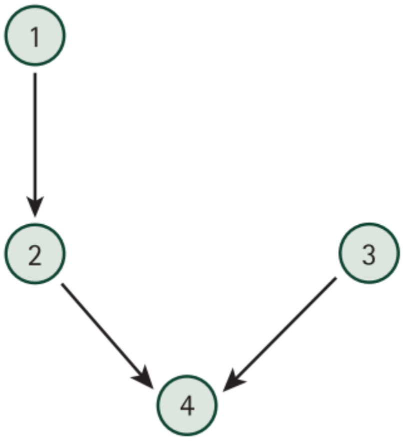


Figure 8.2: Argument diagram (Rainbolt & Dwyer, 2012)

8.5. Argument Diagram: Proposed Access Control Model

In this section, the argument diagram in Figure 8.3 is examined which justifies the inclusion of key components that form part of the proposed model. The development of this argument diagram is based on the content from the study's chapters which was critically evaluated using critical thought. As a result, this argument diagram indicates the logical steps that were taken in order to reach a sub-conclusion as to why the component was included in the proposed model. These logical steps are represented as linked premises that support the sub-conclusion, thus ensuring that the argument is substantiated. For instance, premises [1]-[5] support sub-conclusion [6]. In addition, sub-conclusion [6] as well as no. [16], [23], [28], [33], [39], [43], [48], [53] and [58] also serve as premises that support the conclusion [59]. The conclusion consists of the justifications of the components which make up the proposed model. It is also important to note that some of the sub-conclusions are supported by more than one premise. Sub-conclusion [6] is supported by two premises: [5] and [36]. Sub-conclusion [33] is supported by premises [28] and [32]. Sub-conclusion [39] is supported by premises [6] and [38]. Sub-conclusion [43] is supported by three premises: [39], [42] and [49]. Lastly, sub-conclusion [48] is supported by premises [3] and [47]. The justifications for the selection of the key components of the proposed model, and how they form part of the conclusion, is indicated below:

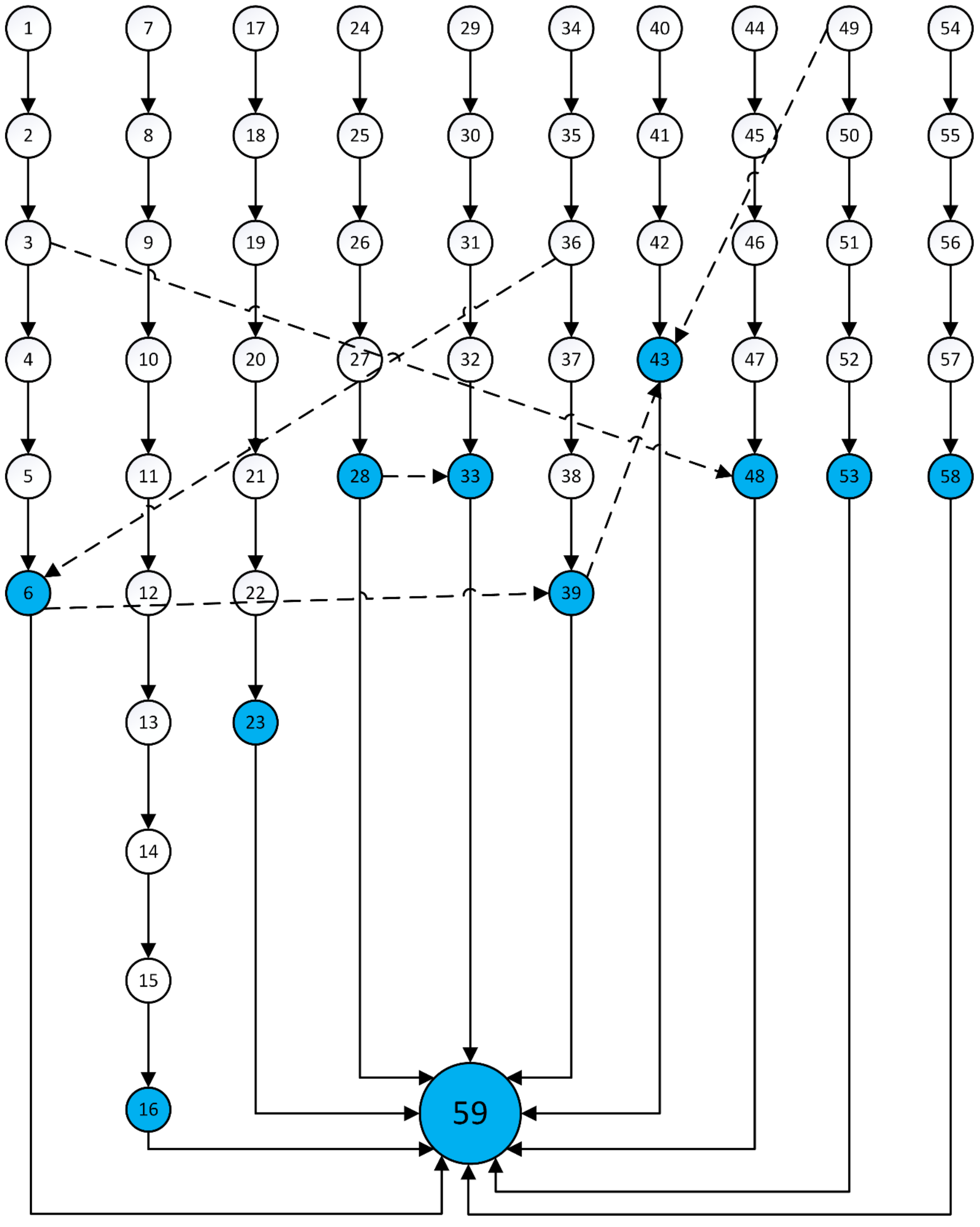


Figure 8.3: Argument diagram justifying choice of proposed model components

[1] The EHR consists of digitally stored health information which represents the patient's lifetime (Canada Health Infoway, 2006c).

[2] Since the EHR represents the patient's lifetime, it is required that the confidentiality of this information is ensured.

[3] However, the EHR should be shared between clinicians in order to treat the patient.

[4] As a result, confidentiality cannot be ensured since access to the patient's EHR by clinicians would violate the patient's confidentiality.

[5] This creates security and privacy issues and if not addressed, this can result in the compromise of a patient's EHR, leading to a loss in patient trust in the national EHR system (Alhaqbani & Fidge, 2007).

Thus,

[6] Access control is needed in order to provide the right level of EHR access to authorised clinicians, while also ensuring the security and privacy of patient information.

[7] Before an entity can access a patient's EHR, they would firstly need to be identified by providing an identifier such as a username (Damon & Coetzee, 2013).

[8] Once an entity has been identified, the provided credentials would need to be verified via an authentication method (Gregg, 2017).

[9] However, each authentication method has a number of disadvantages that can create issues when authenticating.

[10] A number of authentication methods can be used together in order to address these disadvantages and increase the level of security such as SSO, smart card or soft token (Gregg, 2017).

[11] SSO improves user productivity as users only have to remember a single set of credentials (Radha & Reddy, 2012).

[12] A smart card is harder to breach than a password since it cannot be stolen remotely (Abu-Nimeh, 2011).

[13] While smart cards can be used by clinicians to authenticate, patients would need to obtain a smart card reader in order to authenticate.

[14] A soft token i.e. mobile application integrates with the devices that patients already possess such as smartphones (NetIQ, 2016).

[15] Systems requiring a high level of security, such as a national EHR system, should use two or three factors for authentication (Abu-Nimeh, 2011).

Thus,

[16] This study uses two-factor authentication with a combination of a smart card and SSO for clinicians while patients use a combination of a soft token and SSO to authenticate

[17] Clinicians that have been successfully authenticated would then need to be granted the necessary permissions in order to access the EHR via the process of authorisation (Rasiwasia, 2017).

[18] Authorisation is carried out using access control policies (Rasiwasia, 2017).

[19] There a number of access control models, based on different access control policies, which can be used to authorise a clinician.

[20] RBAC can be applied to the healthcare context where users' job functions are based on roles such as a physician (Furnell et al., 2008).

[21] However, RBAC does not support the handling of dynamic events such as an emergency when access to the patient's EHR is needed (Fernández-Alemán et al., 2013).

[22] In spite of this, ABAC can be used to address this drawback of RBAC by supporting dynamic events (INCITS, 2012a).

Thus,

[23] This study uses a combination of RBAC and ABAC for authorisation that draw from two RBAC standards: ANSI INCITS 359-2012 and ANSI INCITS 494-2012, which serve as the theoretical foundation of this study.

[24] The security and privacy of patients' information cannot be ensured by using security controls that only limit access to information (Wickramage, Sahama, & Fidge, 2016).

[25] Through the use of security controls that only limit access to information, such as access control, any misuses of patient information by an authorised clinician would go undetected.

[26] Patient information that is accessed by overriding access control policies, which should only be overridden in an emergency, would also not be detected (Fernández-Alemán et al., 2013).

[27] Additionally, in the event of a data breach, it should be possible to find out what transpired on the affected system (Duncan & Whittington, 2016).

Thus,

[28] Accountability is an essential part of access control that is required in order to ensure that users are held responsible for their actions by tracing actions performed on a system to a user.

[29] Four security models (Chinese wall, Bell-LaPadula, Biba and Clark-Wilson models) were identified, which serve as an application of traditional access control models.

[30] After comparing and contrasting these security models, it was identified that the Clark-Wilson model was the most applicable to this study.

[31] The Clark-Wilson model was created to ensure integrity in a commercial environment (Gregg, 2017).

[32] The concepts of the Clark-Wilson model such as well-formed transactions, authentication, separation of duties and auditing can be applied to a new context other than the commercial environment.

Thus,

[33] This study will be adopting the Clark-Wilson model in the context of a national EHR and also serves as the study's theoretical foundation.

[34] The realisation of a South African national EHR system creates a number of security and privacy risks that patients' EHRs would be susceptible to.

[35] Patient information, contained in EHRs, is at risk of being processed illegally unless rules requiring the lawful processing of patient information are present (DLA Piper, 2018).

[36] Additionally, it is required that patient information is protected through the use of security controls (Botha et al., 2015).

[37] In the event that these security controls are breached and patient information is comprised, it is important that the affected individuals are notified about such a data breach (DLA Piper, 2018).

[38] Organisations that fail to protect or notify patients about the breach of their EHRs need to be held accountable (PoPI Act, 2013).

Thus,

[39] Regulations are needed to ensure that the security and privacy of patients' EHRs are ensured through enforcement and implementation of access control.

[40] South Africa has experienced challenges with regards to a lack of governance in healthcare.

[41] There is a need for strong information governance in order to ensure compliance with essential standards such as security, privacy and interoperability standards (Department of Health South Africa, 2012).

[42] Additionally, regulations and policies need to also be adhered to.

Thus,

[43] Governance is needed in order to ensure that regulations are complied with, policies are established and standards are followed.

[44] The South African national EHR system needs to be based on an EHR system architecture, such as the centralised or distributed architecture, which determines how EMRs will be aggregated in order for the resultant EHR to be accessed nationally.

[45] Notable disadvantages of the centralised architecture include: centralised patient information is not always up-to-date, there is a security risk with centrally storing patient information and the centralised architecture is a single point of failure (AlJarullah & El-Masri, 2013).

[46] The disadvantages of the centralised architecture would have a negative impact on providing healthcare with the EHR as well as creating security risks with the centrally stored patient information.

[47] However, the distributed architecture can address these issues since the latest patient information is available from the health facility where it is located, there is an increased level of security since patient information remains at the source health facility and as a result there is no single point of failure (AlJarullah & El-Masri, 2013).

Thus,

[48] The proposed model has adopted the distributed architecture for providing access to the national EHR.

[49] Many South African health information systems' lack of interoperability has led to a number of disparate systems (Department of Health South Africa, 2012).

[50] Some provinces have health information systems which cannot communicate with other provinces, while some provinces are still paper-based (Ohuabunwa et al., 2016).

[51] As a result, this will not allow the sharing of EHRs between authorised clinicians in different regions.

[52] Additionally, access control and interoperability are linked: without interoperability, access control cannot be enforced on a national EHR system, as this system would not exist without interoperability.

Thus,

[53] Interoperability is essential in order for an interoperable national EHR system to be realised, which will ensure HIE, enabling the sharing of a patient's EHR between authorised clinicians.

[54] The development of the proposed model followed the design science research paradigm.

[55] An important part of design science is that the proposed model should be evaluated according to certain criteria (Hevner et al., 2004).

[56] The evaluation of the proposed model was conducted via an expert review consisting of security and health experts.

[57] All of the expert reviewers were in agreement that the proposed model addresses a relevant research problem.

Thus,

[58] There was consensus from the expert reviewers which indicated that the proposed model's use of access control addressed the research problem.

Thus,

[59] Access control is needed in order to provide the right level of EHR access to authorised clinicians, while also ensuring the security and privacy of patient information. This study uses two-factor authentication with a combination of a smart card and SSO for clinicians while patients use a combination of a soft token and SSO to authenticate. This study uses a combination of RBAC and ABAC for authorisation that draw from two RBAC standards: ANSI INCITS 359-2012 and ANSI INCITS 494-2012, which serve as the theoretical foundation of this study. Accountability is an essential part of access control that is required in order to ensure that users are held responsible for their actions by tracing actions performed on a system to a user. This study will be adopting the Clark-Wilson model in the context of a national EHR and also serves as the study's theoretical foundation. Regulations are needed to ensure that the security and privacy of patients' EHRs are ensured through enforcement and implementation of access control. Governance is needed in order to ensure that regulations are complied with, policies are established and standards are followed. The proposed model has adopted the distributed architecture for providing access to the national EHR. Interoperability is essential in order for an interoperable national EHR system to be realised, which will ensure HIE, enabling the sharing of a patient's EHR between authorised clinicians. There was consensus from the expert reviewers which indicated that the proposed model's use of access control addressed the research problem.

In the next section, the proposed model and its components are covered in more detail.

8.6. Proposed Access Control Model

This section presents the contribution of this study, the proposed access model, by examining each of its components in detail. A number of components have been selected that together address the research problem. The proposed model makes a number of improvements over other national EHR system architectures. Firstly, the IAAA is illustrated and indicates the components of access control that are needed to control access to the national EHR. The available access control models from the literature do not illustrate the use of the IAAA for protecting the national EHR. The proposed model also illustrates how disparate EMRs are aggregated to form the national EHR. Additionally, the proposed model presents the concept of tiered EHRs by indicating how the second tier EHR and first tier EHR are generated with and without the distributed architecture respectively. Also represented in the proposed model is the relationship between regulations and access control which shows how access control is informed by regulations. This is an important relationship that has not been illustrated in the national EHR system architectures of the examined countries. The proposed model in its entirety is illustrated in Figure 8.4.

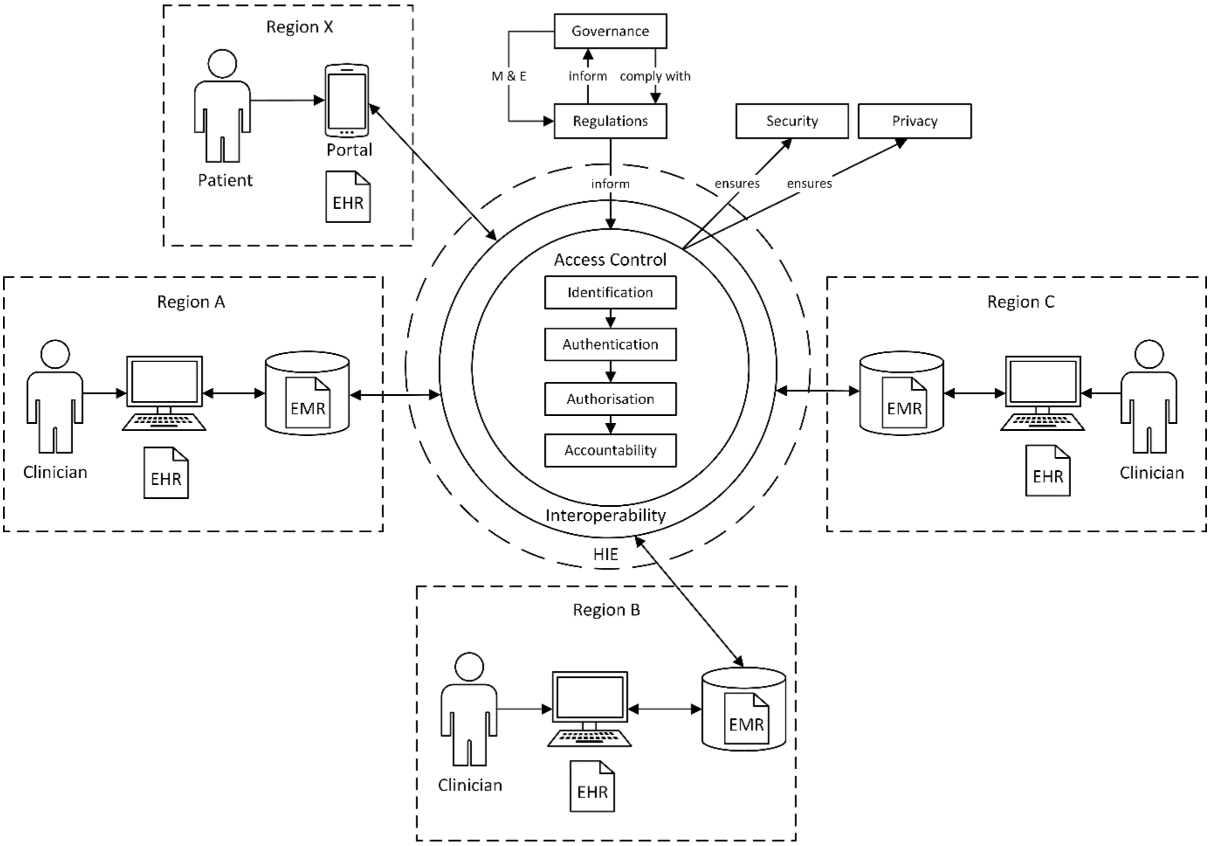


Figure 8.4: Proposed access control model

The discussion of the proposed model begins with covering its use of the distributed architecture for accessing the national EHR. Next, the proposed model presents the first tier and second tier EHRs. This is followed by the application of a TB scenario to the proposed model to indicate how it will operate using a real world healthcare scenario. The proposed model's use of access control for controlling access to the national EHR is then discussed in terms of the IAAA. Next, the theoretical foundation of this study is applied to the proposed model. The regulations component is also covered in terms of how it informs other important components of the proposed model. Lastly, the realisation of interoperability in the proposed model is then presented. The proposed model's use of the distributed architecture for accessing the national EHR is examined next.

8.6.1. Distributed Architecture

The proposed model is based on the distributed architecture. In the distributed architecture, patient information, i.e. the EMR, is stored and managed locally in EMR systems which are located in different health facilities (AlJarullah & El-Masri, 2013). Links containing the location of health facilities where patient information is stored are maintained in the central system. Upon making a request to retrieve a patient's EHR, the central system queries all the health facilities where the patient's information is located. After receiving the patient's information from the EMR systems, all of the patient's information is aggregated by the central system and the result is an EHR which represents all of the health facility encounters made by the patient. The type of patient information that is contained in the retrieved EHR will depend on the clinician's authorisation level. The justification for the use of the distributed architecture over the centralised architecture was covered by premises 44-48 of the argument diagram in Section 8.5. The use of the distributed architecture for realising the national EHR will begin with a discussion using a generic example (Section 8.6.3 applies a TB scenario involving a TB patient's journey to the proposed model).

A patient is admitted to a hospital in Region A. The patient previously visited this hospital and two other health facilities in Regions B and C. The encounters that were made by the patient at these health facilities have been recorded in the EMRs. The retrieval of the patient's EHR by their physician in Region A consists of several steps. Firstly, the physician must be authenticated in order to access the patient's EHR. Links to the patient's EMRs, which are located in different health facilities, are stored in the central system. The central system queries those health facilities where the patient's EMRs are stored. Once these steps have been

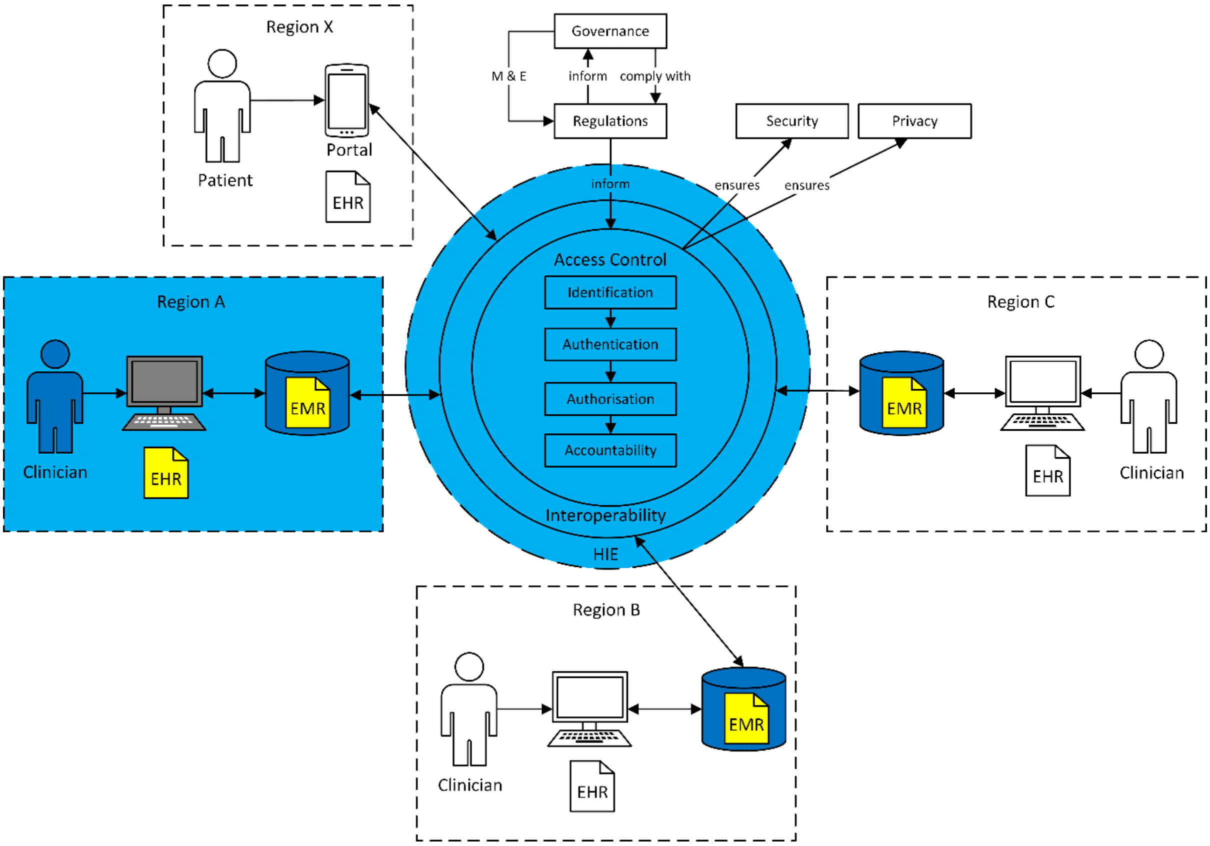


Figure 8.5: Proposed access control model - Retrieval of national electronic health record at Region A

completed, the central system returns the patient's aggregated EHR, which is comprised of the retrieved patient's EMRs located in Regions A, B and C. The bidirectional lines connecting the EMR systems to the interoperability layer indicate how the EMR can either be sent or retrieved via the central system. On the other hand, the bidirectional lines between the clinician's device and EMR system indicate how a clinician can update the EHR (in turn updating the locally stored EMR) or retrieve the EHR. As illustrated in Figure 8.5, the components of the proposed model that take part in this process have been shaded in. This includes the EHR that has been retrieved by the physician in Region A, which comprises of the patient's EMRs from Regions A, B and C.

Unlike the previous example which only focussed on retrieving the EHR, the next example discusses adding information to the EHR, which would consequently be reflected in the retrieved EHR. As depicted in Figure 8.6, after making an observation of the patient, the physician adds new information to the patient's EHR, which is locally stored in the EMR system of the hospital in Region A. Using the distributed architecture, the patient's updated

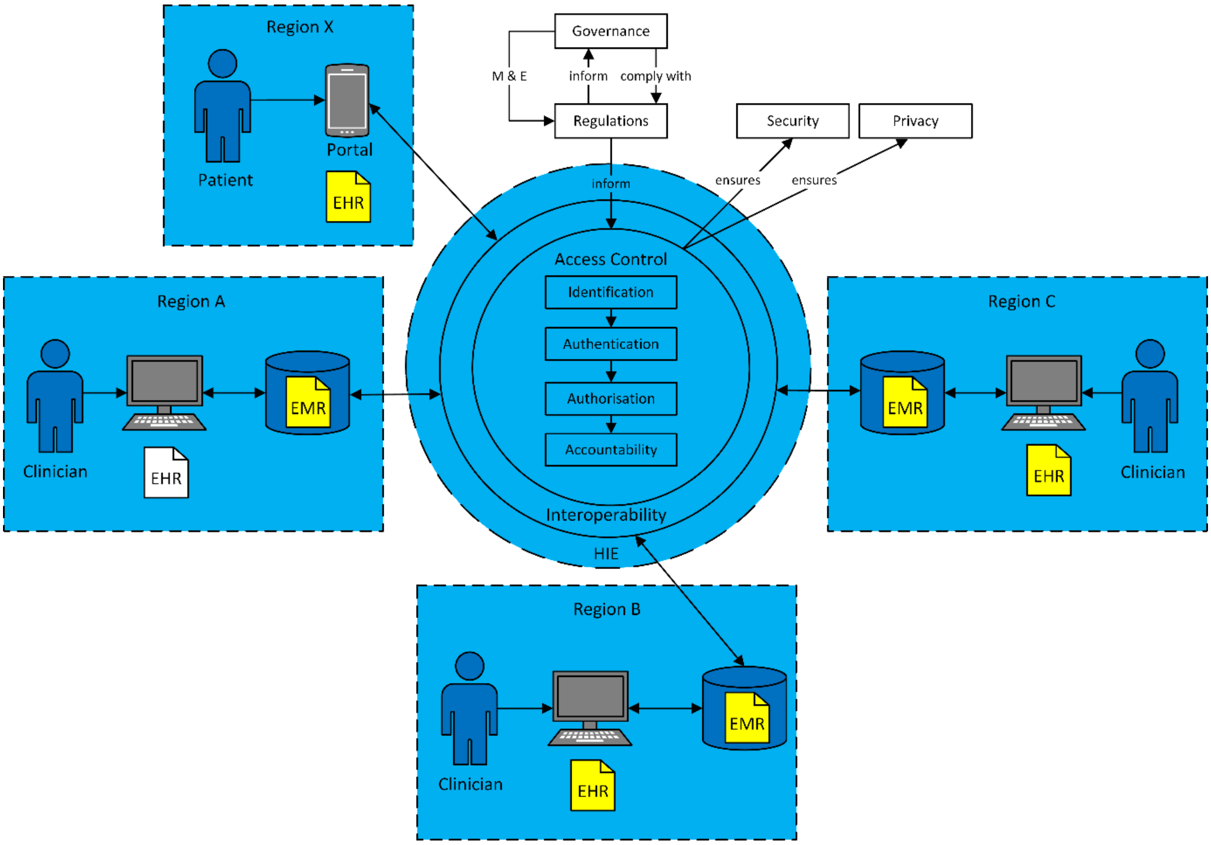


Figure 8.6: Proposed access control model - Retrieval of national electronic health record at Regions B, C and X

EMR is accessible to authorised clinicians in other regions. The EHR is also accessible to the patient through a patient portal which is accessible in Region X i.e. any region in South Africa. The next section presents the concept of tiered EHRs.

8.6.2. Tiered Electronic Health Records

This section presents two terms that have been used to describe two types of EHRs: the first tier EHR and second tier EHR. With regards to the patient's EHR, it is possible for the EHR to be retrieved without the use of the distributed architecture provided that all of the patient's encounters occur within the same health facility. Additionally, the EMR systems that are used by the health facility would be from a single vendor (as discussed in Chapter 7: Section 7.4.1). The study refers to this EHR as a first tier EHR. Figure 8.7 depicts a first tier EHR which has been expanded. As illustrated, the physician, pharmacy and radiology EMR systems are co-located in the same health facility in Region A. The retrieval of the first tier EHR in this instance would not comprise of aggregating EMRs from geographically distributed EMR systems. Instead, the EHR would be accessible locally from the health facility where these EMR systems are also located.

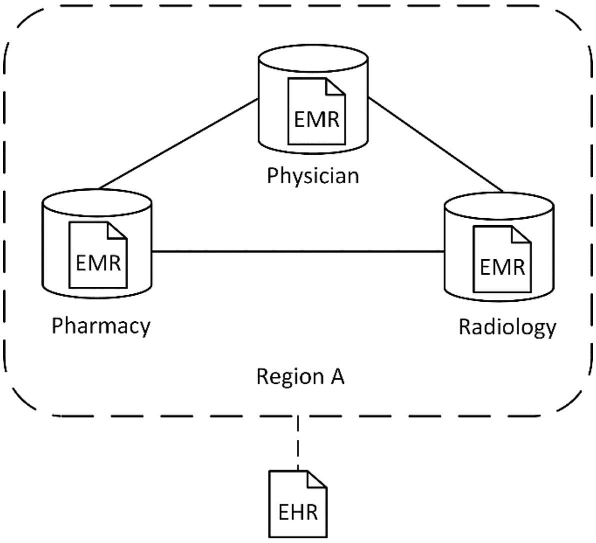


Figure 8.7: First tier electronic health record

In the previous section, the discussion of the proposed model was centred on the use of the distributed architecture for retrieving the aggregated EHR. This study refers to this EHR as a second tier EHR. As illustrated in Figure 8.8, the second tier EHR has been expanded to show its contents. The second tier EHR comprises of the patient's EMRs from Regions A, B and C

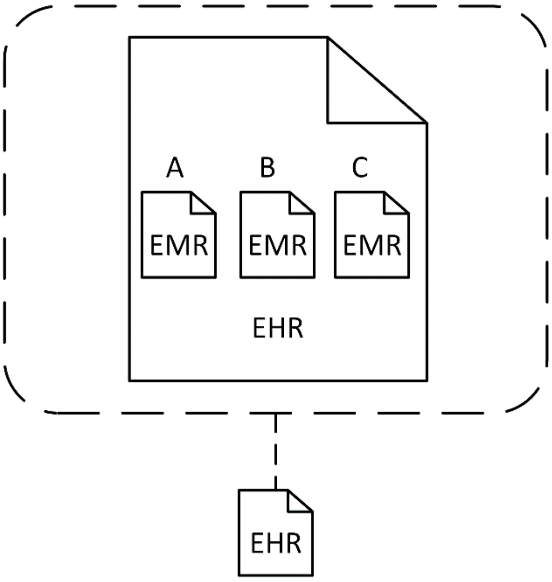


Figure 8.8: Second tier electronic health record

where the patient had previously been treated. Although this study has discussed both first tier and second tier EHRs, this study focusses on the second tier EHR. In the next section, a TB scenario based on the TB disease is applied to the proposed model.

8.6.3. Application of Tuberculosis Scenario to Proposed Model

In this section, a TB scenario comprising of a TB patient's journey is applied to the proposed model. The TB scenario has been adapted from two TB case studies (Ali, n.d.; Kozlov, 2014). The application of the TB scenario is important as it indicates how the proposed model can be used to represent a real world healthcare scenario in the context of a national EHR system. TB has been identified as part of the quadruple burden of disease in South Africa (CSIR & Department of Health, 2014). Thus, the application of the TB scenario to the proposed model is relevant to the South African context. The TB scenario is presented in three parts: testing the patient for TB, the patient diagnosis of TB and patient emergency. The third part of the scenario is also examined in Section 8.6.5.3 from the access control perspective. The entire TB scenario is available in Appendix E. Each part of the scenario consists of points that have been numbered. Points emphasised in bold have been applied to the proposed model in order to link the proposed model to the scenario. The application of these points to the proposed model is illustrated in this section's Figures as orange numbers. The first part of the TB scenario is discussed below.

8.6.3.1. *Testing the Patient for Tuberculosis*

This part of the TB scenario focusses on the testing of a patient for TB. As illustrated in Figure 8.9, this scenario involves two clinicians that are involved in the treatment of Patient A: Physician A and Radiologist A. The testing of Patient A for TB is specified below:

Tuberculosis Scenario Part 1:

1. Patient A is not feeling well and has been experiencing symptoms including a persistent cough and shortness of breath.
2. Patient A visits the local clinic.
3. **Physician A attends to Patient A and retrieves the patient's EHR in order to view their medical history.**
4. **Physician A performs an observation of the patient and records it in the patient's EHR.**
5. **Physician A refers the patient to Radiologist A for a chest X-ray and records this in the patient's EHR.**
6. **Radiologist A retrieves the patient's EHR in order to view the requested chest X-ray from Physician A.**
7. **Radiologist A performs the chest X-ray on Patient A and records the results in the patient's EHR.**

8. **Physician A retrieves the patient's EHR in order to view the result of the chest X-ray.**
9. Physician A finds that Patient A's lungs contain signs of cavities.
10. Physician A sends the patient for a further tests.

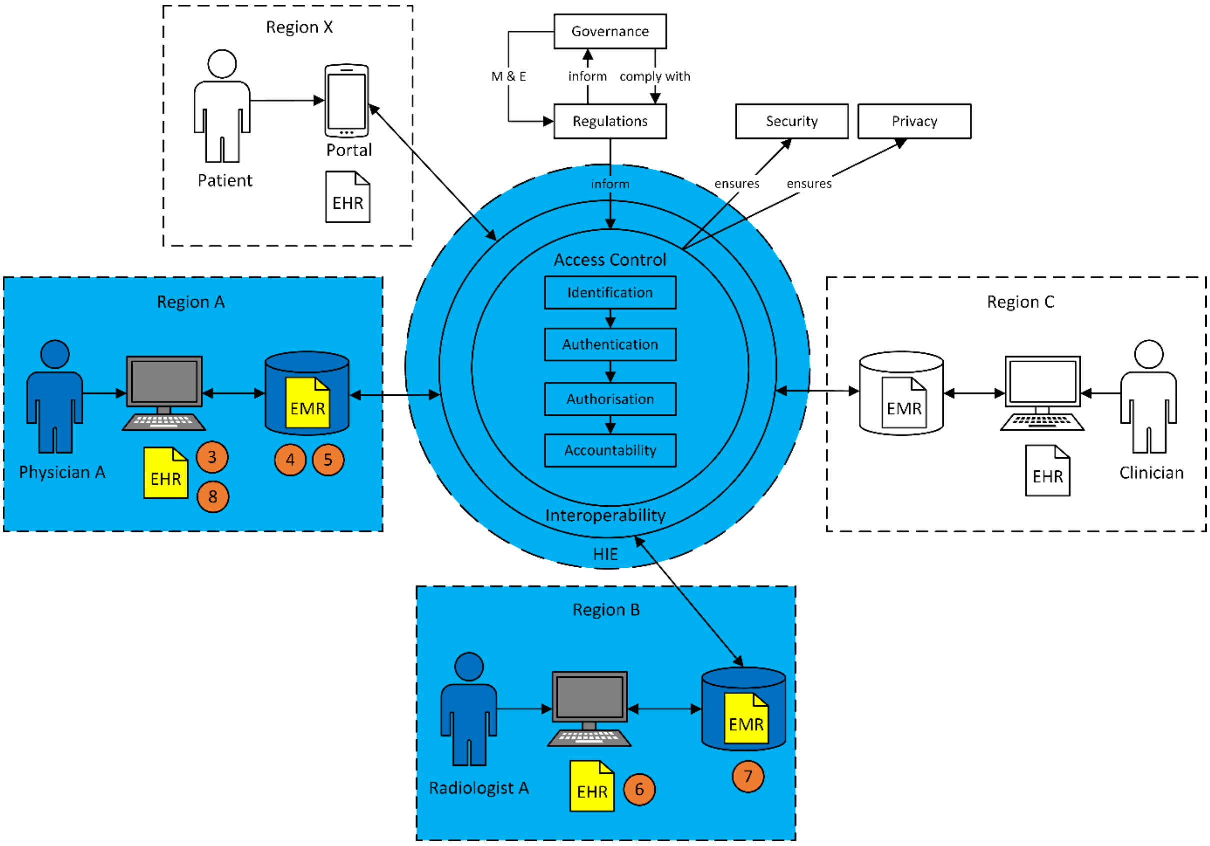


Figure 8.9: Proposed access control model – Tuberculosis scenario part 1

Regarding points 4, 5 and 7, where Physician A and Radiologist A have updated the patient's EHR, it is important to note that the updated information is stored in the local EMR systems in Regions A and B. The updated EHR that is retrieved by Physician A (point 8) includes the patient's chest X-ray results from the EMR system of Radiologist A. This is made possible by the distributed architecture which aggregates the EMRs originating from the EMR systems of Physician A and Radiologist A. The second part of the TB scenario is covered next.

8.6.3.2. *Patient Diagnosis of Tuberculosis*

The second part of the TB scenario covers the patient's diagnosis of TB. As depicted in Figure 8.10, three clinicians are represented in this scenario: Physician A, Pathologist A and Pharmacist A. The involvement of these clinicians in the treatment of Patient A is discussed below:

Tuberculosis Scenario Part 2:

11. **Pathologist A analyses Patient A's test results and records the results in the patient's EHR.**
12. After a few days, Patient A returns to the clinic to find out their test results.
13. **Physician A views the patient's EHR and informs them that they have contracted TB.**
14. **Physician A prescribes medication for the patient and records it in the patient's EHR.**

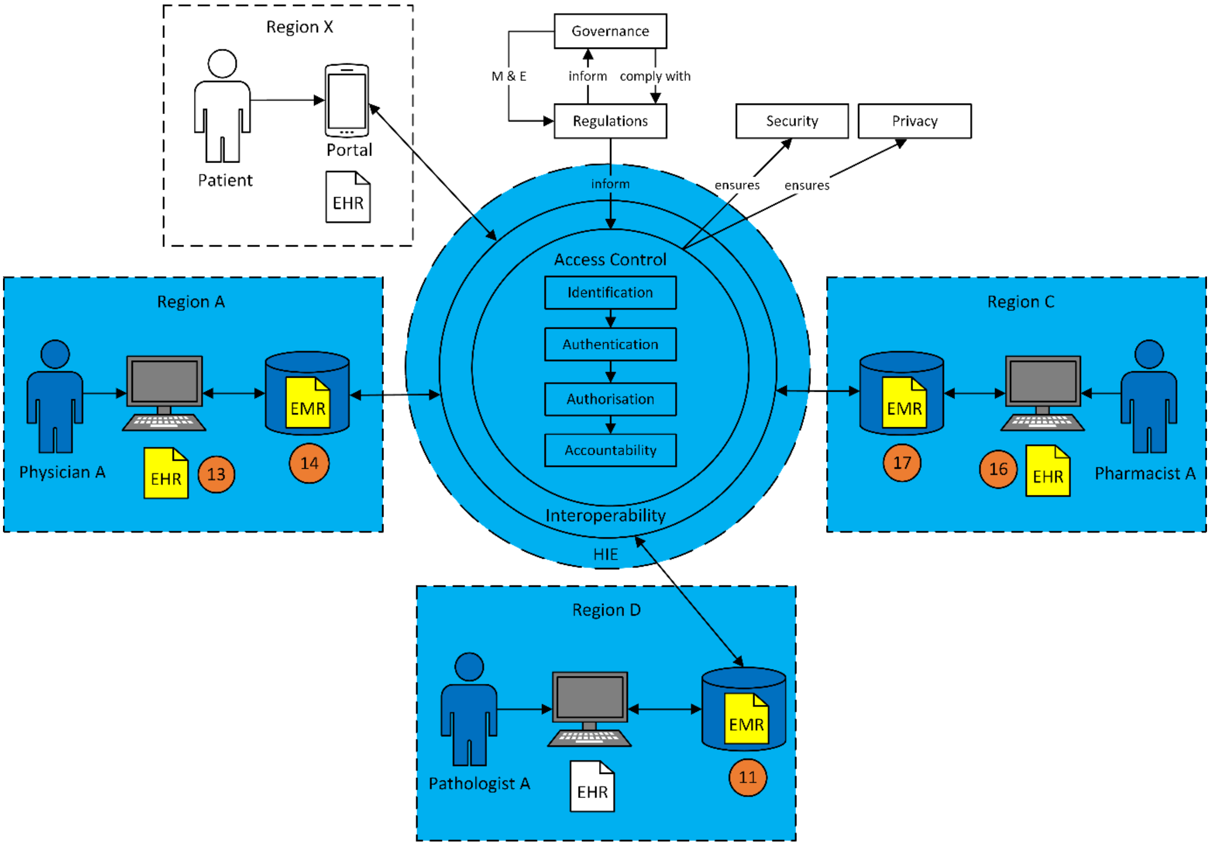


Figure 8.10: Proposed access control model – Tuberculosis scenario part 2

15. Patient A goes to the pharmacy to collect their medication.
16. **Pharmacist A retrieves the patient's EHR to view their prescription.**
17. **Pharmacist A gives the patient their medication and records this in the patient's EHR.**

With regards to point 13, the EHR that is retrieved by Physician A includes the patient's test results from Pathologist A's EMR system in Region D. While not illustrated in Figure 8.10, the EHR also includes the patient’s chest X-ray results from the EMR system of Radiologist A in Region B (which was discussed in the previous section). The final part of the TB scenario is examined next.

8.6.3.3. *Patient Emergency*

This section covers an important part of the TB scenario which describes an emergency event involving a TB patient. This part of the scenario is revisited in Section 8.6.5.3 which discusses it from an access control perspective. Figure 8.11 depicts two clinicians that take part in this scenario: Physician B and Nurse A. The emergency event involving the TB patient is examined below:

Tuberculosis Scenario Part 3:

18. After a few months since being diagnosed with TB, Patient A, who is unconscious, is transported to the emergency department.
19. Physician B, who is working in the emergency department, does not have access to the patient’s EHR.
20. Since this is an emergency, Physician B gains access to the patient’s EHR by using the break-glass feature.
21. **Physician B retrieves the patient’s EHR to view the patient’s medical history.**
22. **Physician B performs an observation of the patient and appends it to the patient’s EHR.**
23. Physician B transfers the patient to be admitted in the local hospital.
24. **Nurse A checks and records the patient’s vital signs in the patient’s EHR.**

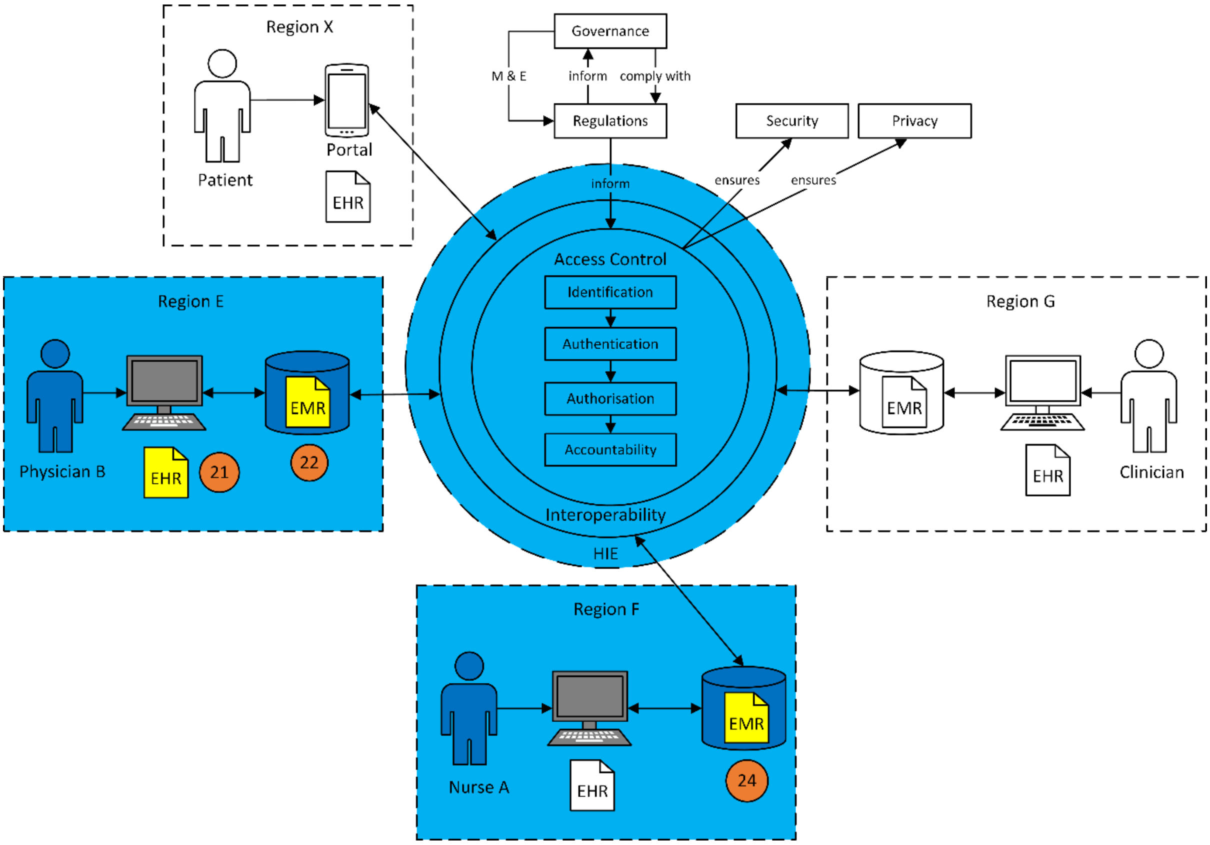


Figure 8.11: Proposed access control model – Tuberculosis scenario part 3

At the end of the third scenario, a request for the retrieval of Patient A's EHR would comprise of the EMRs that were updated by a number of clinicians throughout the scenario: Physician A, Radiologist A, Pathologist A, Pharmacist A, Physician B and Nurse A. It is evident that an increasing number of clinicians have access to the patient's EHR. This would need to be controlled using access control and is discussed in the next section.

8.6.4. Access Control: Overview

In the previous sections, the proposed model was covered from the health information systems perspective and indicated how a patient's national EHR can be accessed by clinicians who are involved in the treatment of the patient. From the discussion of the TB scenario it is evident that through the use of the national EHR, the patient's information is accessed by a large number of geographically distributed clinicians, which included Physician A, Radiologist A, Pathologist A, Pharmacist A, Physician B and Nurse A. Thus, access control is an essential component of the proposed model that is required in order to control access to the patient's EHR.

By controlling access to the patient's EHR, it is important that clinicians are authorised to access those parts of the EHR that are relevant to their function. This ensures that clinicians are not given access to all of the information in the patient's EHR as this would create risks to the security and privacy of the patient's EHR. Based on the principle of 'least privilege', the clinician should only be able to perform the minimum operations that are needed on a patient's EHR (Whitman & Mattord, 2016). For example, referring to the TB scenario from Section 8.6.3, Pharmacist A should be able to view the prescription information in Patient A's EHR in order to provide them with medication but should not be able to delete this information. While Pharmacist A can view the prescription information of Patient A, they should not be able to view the patient's medical history. On the other hand, Physician A would be authorised to access Patient A's medical history as this information is needed in order to treat Patient A. Hence, through the use of access control, each clinician involved in the care of Patient A would have a different level of access to the patient's EHR based on their job function. RBAC, which enables the principle of least privilege, was discussed in Chapter 5: Section 5.4.4.

While the study focusses on controlling clinician access to the patient's EHR, the proposed model also illustrates how patients would have access to their EHR via a patient portal. Chapter 3: Section 3.5.4 (under New Zealand and Sweden) discussed how clinicians may not agree with patients having access to certain health information in their EHR. This is because a patient that has contracted a new disease may not understand the impact of the disease without the consultation of their physician. Additionally, giving patients full permissions on their EHR would create security and privacy risks. This would allow patients to inadvertently modify or delete their personal information. As a result, the patient portal in the proposed model allows the patient to have read access to certain sections of the EHR that would be useful to them. For example, patients would be allowed to view the section of the EHR that lists the medication that they have been prescribed, which would assist the patient in the event that they forget the medication that they are taking. In order to access the EHR, both patients and clients use two-factor authentication to authenticate to the EHR. However, while clinicians will need to authenticate to the EHR using a combination of a smart card and SSO (as discussed in Section 8.6.5.2), patients will use a combination of a soft token, i.e. mobile application which will generate OTPs, and SSO to authenticate. Unlike clinicians, patients use a soft token instead of a smart card since patients would need to obtain a smart card reader in order to authenticate. Additionally, soft tokens integrate with the devices that patients already possess such as smartphones (NetIQ, 2016). In the next section, the IAAA is applied to the proposed model.

8.6.5. Access Control: IAAA

In this section, the components of access control i.e. identification, authentication, authorisation and accountability are discussed in terms of the proposed model. An expansion of the authentication and authorisation components is also illustrated which indicates in detail how the clinician is authenticated and authorised to access the patient's EHR. The use of accountability in both the authentication and authorisation components is also covered. The authorisation component also discusses how the proposed model can handle emergency events through the application of Part 3 of the TB scenario, which was covered in Section 8.6.3.3. Firstly, identification of the clinician in the proposed model is discussed.

8.6.5.1. *Identification*

During the identification stage, the clinician would need to identify themselves to the system by providing an identity in the form of a smart card. In order to proceed, the identity of the clinician would need to be verified using authentication. The proposed model's use of authentication for authenticating clinicians is covered below.

8.6.5.2. *Authentication*

Once the clinician has provided their identity by inserting their smart card, this identity would need to be verified via authentication. The proposed model uses two-factor authentication comprising of a smart card and SSO. This was chosen over two-factor authentication consisting of biometrics (fingerprint) and SSO since the use of biometrics would act as a barrier to clinicians that wear clinical gloves. Figure 8.12 illustrates a flowchart indicating how clinicians are authenticated via the authentication component in the proposed model. The flowchart visually represents the process of authentication in the proposed model using a number of steps. The first step checks if a SSO session is already active i.e. if the clinician has already been authenticated. If the clinician has already been authenticated, they are granted access to the EHR. The benefit of SSO is evident when the clinician later wants to access another eHealth application as they will not be prompted to reauthenticate. The successful access to the EHR or another eHealth application is logged as indicated by the 'Log successful access' step. If an active SSO session is not found, the clinician is prompted to authenticate using a smart card and SSO. Firstly, the clinician inserts their smart card into the smart card reader. The clinician is then prompted for their SSO credentials. If the submitted credentials are valid, the clinician is granted access to the EHR. However, if incorrect SSO credentials are submitted, access is denied and this is logged as indicated by the 'Log failed access' step. Once

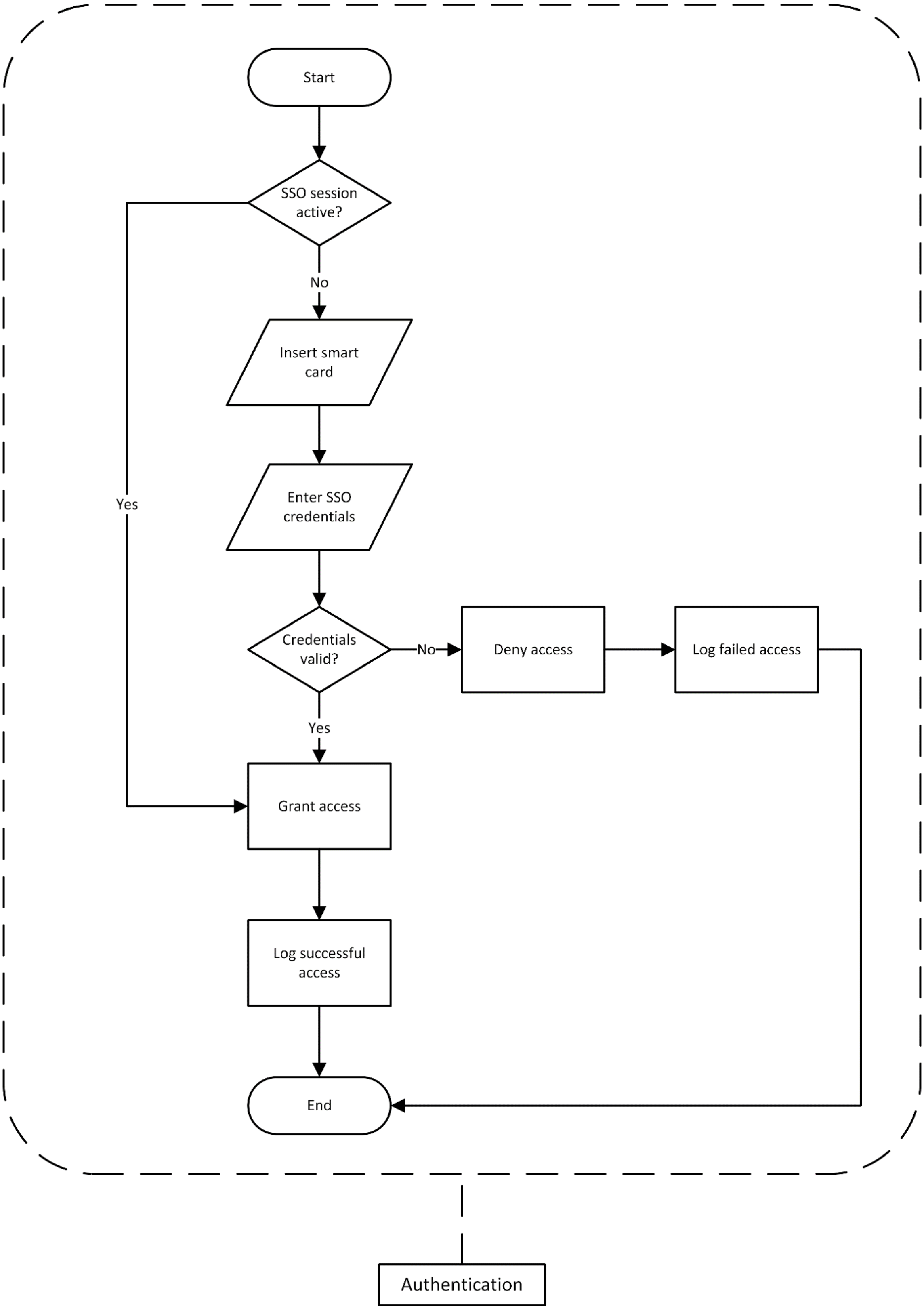


Figure 8.12: Flowchart of clinician authentication using two-factor authentication

the clinician has been authenticated, they would be granted certain permissions to the EHR based on the verified identity, which is discussed next under authorisation.

8.6.5.3. *Authorisation*

Once the identity of the clinician has been authenticated, the clinician would need to be granted certain permissions in order to access the patient's EHR. The proposed model uses a combination of RBAC and ABAC for making access control decisions, which forms part of the studies theoretical foundation (as discussed in Section 8.6.6). The proposed model's use of RBAC and ABAC is illustrated in Figure 8.13 which focusses on the authorisation component of the proposed model. This flowchart depicts the steps that are taken during the process of authorisation. With regards to RBAC, the role that has been assigned to the authenticated clinician is activated. For instance, the physician role would be activated if the authenticated clinician is a physician. The activated role should follow the principle of least privilege which would ensure that the minimum set of permissions are granted to the clinician for performing their job function. The activation of this role is then logged as a successful authorisation. Although the clinician has been granted the necessary permissions to perform their job function via RBAC, RBAC cannot grant the clinician exceptional permissions in the event of an emergency. The proposed model addresses this limitation through the use of ABAC during the 'Emergency physician?' step. Through the use of ABAC, this step checks if the authenticated clinician is an emergency physician: if the clinician is a physician (via the position attribute) and is located in the emergency department (via the location attribute), then the break-glass feature would be available to the clinician. A purpose of use attribute also exists for specifying patient consent that will determine whether the clinician has access to a specific patient's EHR.

The proposed model's authorisation component is also expanded in Figure 8.14 to illustrate a flowchart indicating the steps to be taken in order gain emergency access via the break-glass feature. As mentioned earlier on, only emergency physicians would have access to the break-glass feature since their job function would require it. Thus, when the same physician is not working in the emergency department, they would not have access to the break-glass feature. With regards to the third scenario in Section 8.6.3.3, Physician B has received an unconscious patient that they have not treated before. Thus, patient consent would not have been provided. In order to gain access to the patient's EHR, in the interests of the patient's health, Physician B accesses the break-glass page. The break-glass page indicates to the clinician that all

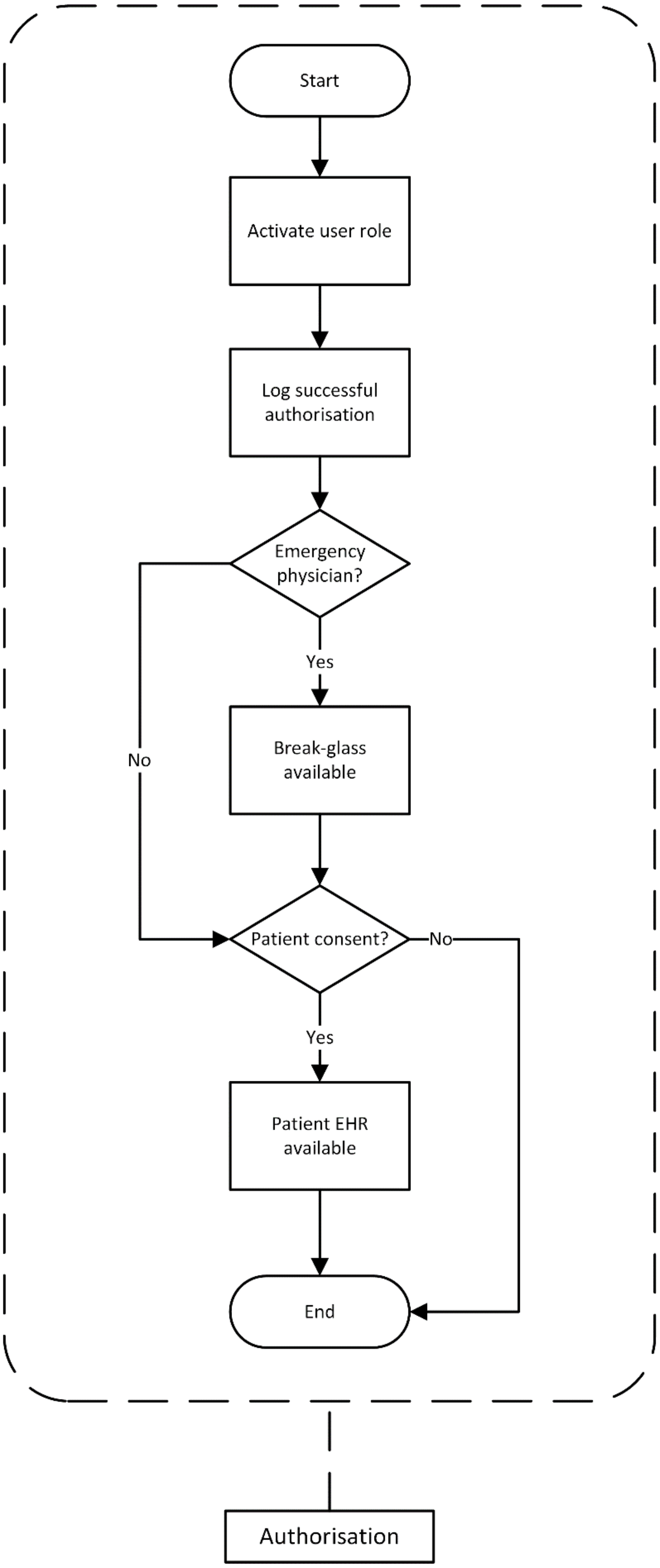


Figure 8.13: Flowchart of clinician authorisation using RBAC and ABAC

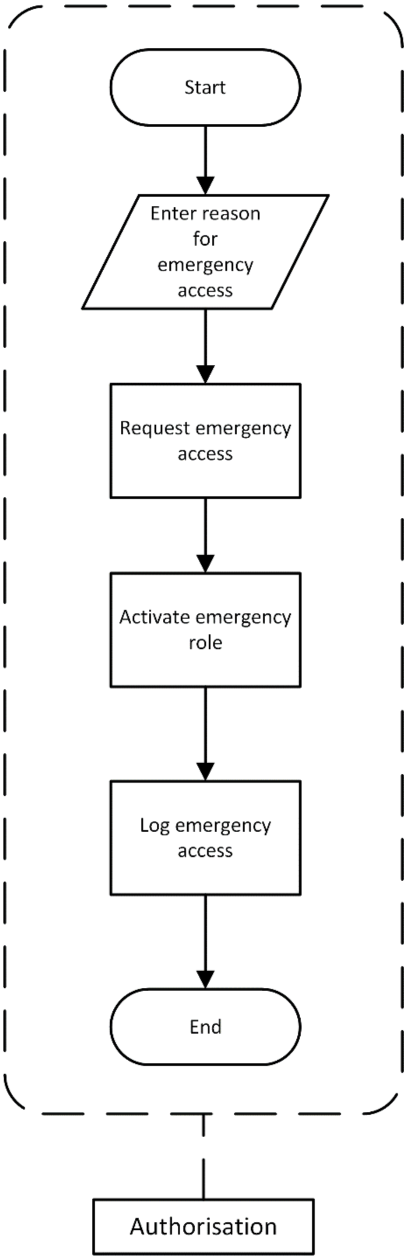


Figure 8.14: Flowchart of clinician requesting emergency access

subsequent actions on the patient's EHR will be logged. This message serves as a deterrent to any clinicians who may attempt to access the patient's EHR in a non-emergency situation. Next, Physician B enters a reason for the emergency access and this is used as the purpose of use attribute via ABAC. Physician B then requests emergency access by submitting the reason to the system. Next, the emergency role is activated for Physician B and the physician now has access (only read and append permissions) to the patient's EHR. It is important to note that this emergency access is logged and all actions made by Physician B will be recorded and audited. Once Physician B is done with the patient's EHR, the emergency role is deactivated.

The proposed model's use of accountability for holding clinicians accountable, for their actions on the patient's EHR, is covered next.

8.6.5.4. *Accountability*

The accountability component has been included in the proposed model since it is an important part of access control which ensures that users are held responsible for the actions that they perform on the patient's EHR. As discussed in Chapter 5: Section 5.7.1, accountability i.e. auditing should be performed in response to a data breach as well as when the patient requests to view their audit trail in order to monitor who has accessed their EHR. Thirdly, auditing should be performed by using a risk-based approach that would detect access to the EHR which poses the greatest risk to patient information such as EHR access from an unknown location. The fourth but essential type of auditing involves monitoring all EHR accesses that result from the request of emergency access. As discussed earlier on, this type of EHR access would occur when a clinician requests emergency access via the break-glass feature. In the event of this exceptional access, the patient should be notified as well as the EHR custodian who would need to audit the emergency access in order to determine whether it was legitimate or not. The presence of the break-glass feature is dependent on the accountability component. This is because without the accountability component, the break-glass feature could be abused without anyone being held accountable. Unlike the other three components of the IAAA that are executed one after the other i.e. identification, authentication then authorisation, the execution of the accountability component does not depend on whether the previous three components of the IAAA are executed. For instance, the accountability component is executed during the authentication of the clinician (as illustrated in Figure 8.12) where the accountability component would log whether the authentication was successful ('Log successful access') or not successful ('Log failed access'). With regards to authorisation, the accountability component would also be executed when the clinician's role is activated ('Log successful authorisation' as depicted in Figure 8.13) as well when the clinician requests emergency access via the break-glass feature ('Activate emergency role' as illustrated in Figure 8.14). Furthermore, any operations performed on the patient's EHR including create, read, write and append permissions would also be recorded in the audit trail. In the next section, the proposed model is discussed in terms of how it adopts the ANSI RBAC standards for controlling access to the EHR.

8.6.6. Theoretical Foundation: ANSI Role-Based Access Control Standards

As discussed in Section 8.6.5.3, the proposed model uses a combination of RBAC and ABAC for making access control decisions. This is made possible by the proposed model's adoption of two ANSI RBAC standards: ANSI INCITS 359-2012 and ANSI INCITS 494-2012 (which were discussed in Chapter 5: Section 5.5). ANSI INCITS 494-2012 specifies dynamic attributes which have been used in the proposed model such as position, location and purpose of use (patient consent and emergency access). With regards to the components of ANSI INCITS 359-2012, the proposed model implements core RBAC, hierarchical RBAC and constrained RBAC. Additionally, the proposed model's use of the RBAC system and administrative functional specification is also covered.

In core RBAC, permissions are assigned to a role and users gain those permissions by being assigned to the role. For instance, the physician role would be assigned permissions, following the principle of least privilege, such as create, read, write and append permissions on the patient's EHR. A physician would then be assigned the physician role and gain those permissions. Sessions are also included in core RBAC where a user's roles would be activated. For example, a physician who sometimes works in the emergency department may also be assigned an emergency role but this emergency role will only be activated when the physician has executed the break-glass feature in the event of an emergency. The proposed model uses limited role hierarchies from hierarchical RBAC which enable roles to inherit permissions from another role. For instance, both the physician and nurse roles could inherit permissions from the employee role. As a result, common permissions would not need to be added manually. The proposed model implements constrained RBAC through the use of DSD, which is executed by the authorisation component. Using DSD, no user would be able to activate conflicting roles simultaneously. For example, an administrator may be assigned two roles: one that allows them to create user accounts (for accessing the EHR) and another role that allows them to approve the creation of user accounts. Through the use of DSD, an administrator would not be able to both approve and create the same user account but would be able to approve the user accounts which have been created by other administrators. DSD would also prevent the same administrator from approving and creating privileged user accounts which could allow the administrator to compromise patients' EHRs. With regards to the RBAC system and administrative functional specification, this component includes administrative commands such as the creation and management of users. This would enable the creation of user accounts for new clinicians while also revoking access for clinicians that have left an organisation, which is important for ensuring that access is only given to those that require it for their job. Administrative review functions are also included with the RBAC system and administrative functional specification, which can be used to find out if a specific clinician has been granted excessive permissions. Lastly, system functions are included for the creation of user sessions and for making access control decisions. For example, for an authenticated clinician, these functions would activate the clinician's role within a session as well as check if the clinician's activated role would have the required permissions to access the patient's EHR. Next, the proposed model's adoption of the Clark-Wilson model is discussed.

8.6.7. Theoretical Foundation: Clark-Wilson Model

This section discusses how the proposed model incorporates concepts from the Clark-Wilson model, which was originally created to ensure integrity in a commercial environment (as discussed in Chapter 5: Section 5.6.4). The Clark-Wilson model has been adopted in the context of a national EHR system. The proposed model has incorporated the concepts of the Clark-Wilson model including well-formed transactions i.e. TPs, authentication, separation of duties and auditing.

Figure 8.15 illustrates how well-formed transactions are ensured: the clinician in Region A can only modify the information contained in the patient's EHR i.e. CDI (which is stored in the EMR) through the intermediary application (TP) which is running on their device. Integrity is ensured since modification of the patient's EHR is done through the intermediary application which constrains what the clinician can do with regards the patient's EHR. As a result, the clinician would not be allowed to directly modify the data through other means other than through the application that they are authorised to use. In order to legitimately update patient information, the clinician would enter the new data via the application. Under the Clark-Wilson model, this new data i.e. UDI cannot be added to the EHR in its raw form as this would create risks to the integrity of the patient's EHR. Before the new data is added to the EHR, it would first need to be validated and transformed into a CDI. For example, before a physician can enter an observation into a patient's EHR, this new data would need to be validated by the TP and then transformed into a CDI. The Clark-Wilson model also specifies the use of authentication which was covered by the proposed model in Section 8.6.5.2. Here, before a clinician can execute a TP to update a patient's EHR, their identity must first be authenticated. Since the Clark-Wilson model is based on roles, the well-formed transactions that a clinician can execute will depend on the assigned role. For example, a nurse may be allowed to execute 'update patient vital signs' transaction but only the physician would be able to execute the ‘create prescription’ transaction. Similar to the previously discussed ANSI RBAC standards in Section 8.6.6, the Clark-Wilson model also includes separation of duties which is enforced by splitting TPs i.e. well-formed transactions between users so that no single user would exceed their authorisation level which would result in unauthorised modifications of data. The Clark-Wilson model, like the proposed model, also focusses on auditing the actions of users. For instance, a clinician that executes the ‘write observation’ transaction on a patient’s EHR, would have their actions appended to the audit trail in the form of a CDI.

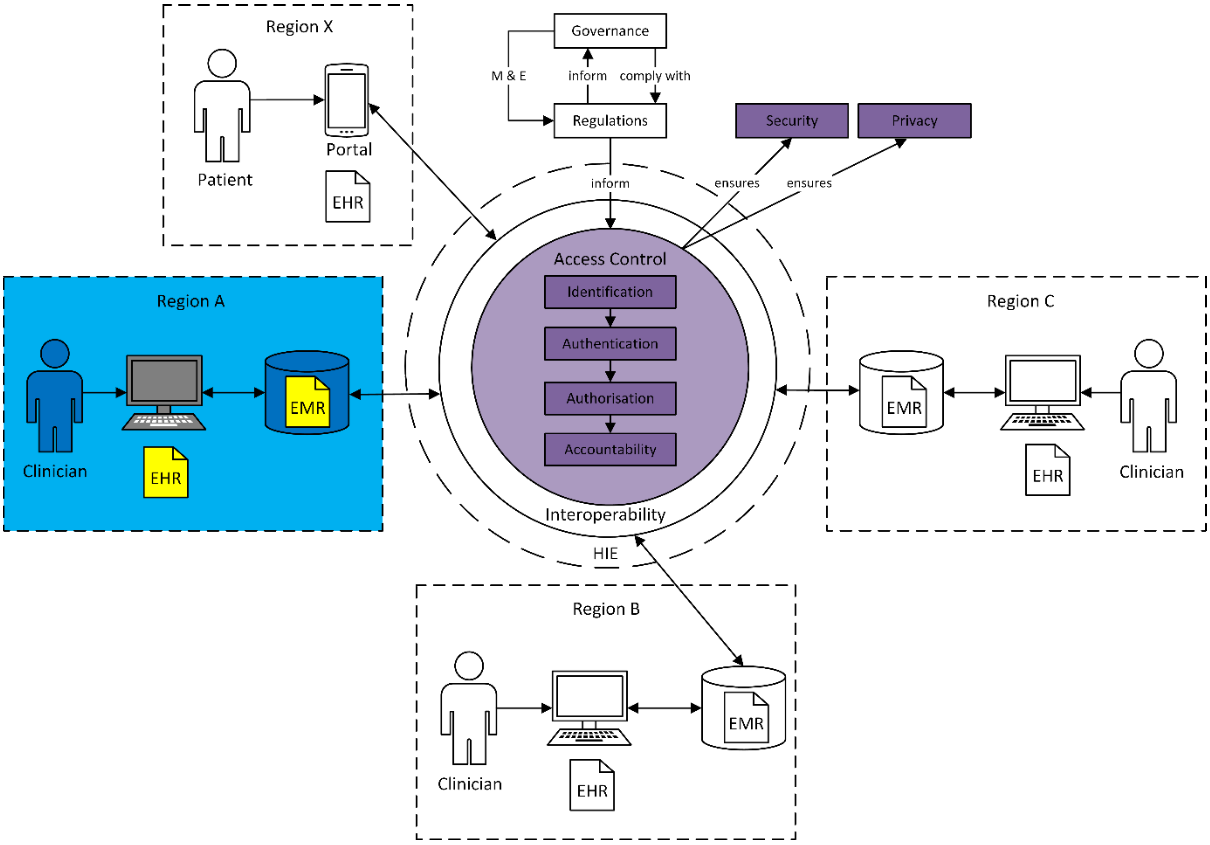


Figure 8.15: Proposed access control model - Theoretical foundation

As discussed in the previous sections, the proposed model’s use of access control for ensuring the security and privacy of a patient’s EHR was covered including how the theoretical foundation of the study achieves this. Using Figure 8.15, it can be justified how access control ensures security and privacy. Security is ensured through access control, which maintains the confidentiality and integrity of the EHR. Access control ensures confidentiality by ensuring that certain patient information contained in the EHR is not disclosed to unauthorised entities. Additionally, integrity is also ensured since the patient’s information would only be modified by authorised clinicians. It is evident from the discussion of the theoretical foundation that RBAC ensures both confidentiality and integrity while the Clark-Wilson model ensures integrity. With regards to privacy, the proposed model's use of RBAC ensures this through the principle of least privilege, thus preventing clinicians from accessing more patient information than they need to do their jobs. In addition, medical emergencies which cannot be handled by RBAC are handled by ABAC. ABAC provides exceptional access for a limited period which is also audited. Regulations, which also assist in ensuring patient privacy, are covered in the next section.

8.6.8. Regulations

Regulations is an important component of the proposed model which will determine how access control operates in order to control access to the patient's EHR. In the context of a South African national EHR system, the PoPI Act (which was discussed in Chapter 4: Section 4.2.3) would be the most relevant regulation for ensuring the security and privacy of the patient's EHR. The conditions of the PoPI Act (2013), which have been applied to the proposed model, are discussed in this section. The PoPI Act indicates that the confidentiality and integrity of personal information must be ensured through the use of security controls. The proposed model ensures the confidentiality and integrity of personal information through the use of access control. In addition, the PoPI Act specifies that the processing of personal information can only take place if the subject i.e. patient provides their consent, which would allow authorised clinicians to access the patient's EHR. The verification of patient consent is made possible by ABAC's purpose of use attribute as discussed in Section 8.6.5.3. Thus, it is evident that regulations inform how access control will function. Also mentioned in the PoPI Act is that the processing of personal information may only be conducted if it protects a legitimate interest of the subject e.g. the treatment of the patient. This rule is supported by the proposed model which uses the break-glass feature and the purpose of use attribute (via ABAC) for granting emergency access to the patient's EHR when the patient is unconscious and unable to provide their consent.

The relationship between regulations and the other components of the proposed model, such as access control, is illustrated in Figure 8.16. While the bottom part of the figure originates from the proposed model, the top part of the figure provides an alternate view with the addition of components such as standards and policies. The central location of regulations in Figure 8.16 emphasises the importance of regulations which inform the other components: governance and management, policies, standards and access control. It is important to note that regulations indirectly ensure the security and privacy of the EHR through access control. This is because the manner in which access control operates is informed by regulations. Governance and management must comply with regulations and do so by establishing policies and following standards. The policies component consists of access control policies which inform access control since these policies will determine how access control decisions will be made. Policies are also informed by standards such as security (ISO/IEC 27001) and privacy (ISO/IEC 29100) standards, which were discussed in Chapter 4: Section 4.5. In addition to regulations and policies, security and privacy standards also inform how access control will function. An essential part of Figure 8.16 is that it indicates that governance and management must monitor and evaluate compliance with regulations. This would include periodically verifying whether

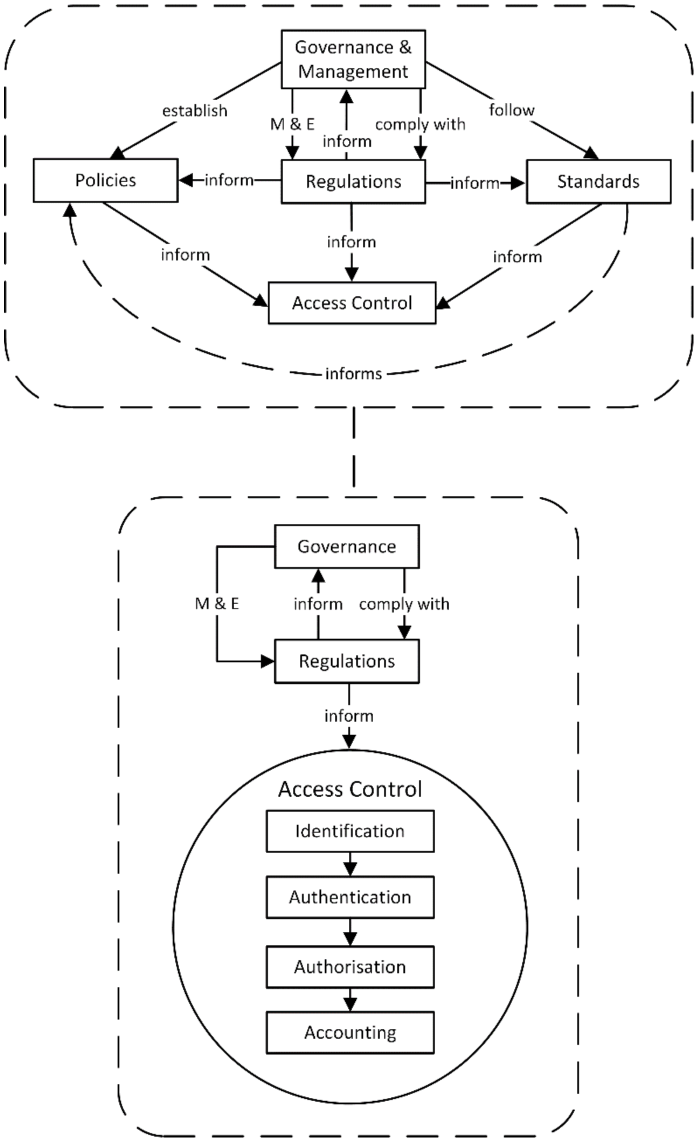


Figure 8.16: Alternate view showing relationship between regulations and other components

security controls, such as access control, are effectively functioning according to access control policies so that the security and privacy of patients' EHR is ensured. In addition to security and privacy standards, governance and management should also follow interoperability standards in order to realise an interoperable national EHR system. The interoperability component of the proposed model is discussed next.

8.6.9. Interoperability

The interoperability component has been included in the proposed model since the realisation of a national EHR system is dependent on the interoperability of disparate EMR systems. Additionally, without interoperability, access control cannot be enforced on a national EHR system since a national EHR system would not exist without interoperability. Figure 8.17 illustrates an alternate view of the proposed model comprising of the interoperability view (the access control component has been condensed). In this view there are four registries which are connected to the interoperability layer: TR (Terminology Registry), PR (Patient Registry), HPR (Health Provider Registry) and FR (Facility Registry). The role of these registries in HIE is covered in this section.

The proposed model ensures all three levels of interoperability: foundational, syntactic and semantic interoperability, which were covered in Chapter 6: Section 6.2. These three levels of interoperability are ensured by the interoperability layer which functions as a HSB. The interoperability layer enables foundational interoperability by connecting the disparate EMR systems together in a network, which allows these systems to exchange information with one another. Syntactic interoperability is also enabled since the interoperability layer also functions as an interface which transforms the exchanged messages, between two disparate EMR systems, into a common standardised format. For example, an HL7 v2 message which is sent by EMR system A to EMR system B would not be recognised if EMR system B were using the HL7 v3 standard. By functioning as an interface, the interoperability layer can transform the sent HL7 v2 message into HL7 v3 format which will be recognised by EMR system B and vice a versa. Semantic interoperability is ensured through the use of the terminology registry. The terminology registry is able to map between different terminology standards such as SNOMED CT and ICD-10. In order to map the terminology contained in the sent message from EMR system A, the interoperability layer calls the terminology registry which maps the terminology to a standardised terminology. The standardised terminology can then be mapped by the terminology registry to a terminology that EMR system B, the receiving system, understands. By ensuring all three levels of interoperability, the interoperability layer enables

HIE. This allows health information to be exchanged between health facilities in different regions. HIE has been positioned at the outermost layer in the proposed model to emphasise how HIE enables the sharing of health information to the surrounding regions. In addition, the HIE layer uses dotted lines to indicate that while it is at the outermost layer of the model, EMR systems interface directly with the interoperability layer.

Registries including the patient registry (also referred to as a PMI), health provider registry and facility registry play an important role in HIE. This is evident as registries have been included in the national EHR system architectures of the five examined countries (as discussed in Chapter 3: Section 3.4.3). These registries store and maintain information which is required to uniquely identify entities in the EHR: the patient registry uniquely identifies patients, the health provider registry uniquely identifies healthcare providers and the facility registry uniquely identifies the locations of care. Before the patient's EMRs from different health facilities can be aggregated, it is important that the patient registry uniquely identifies the patient so that a unique identifier (such as the South African ID number) can be used to identify the patient across all health facilities. This will ensure that the aggregated EHR is comprised of all the

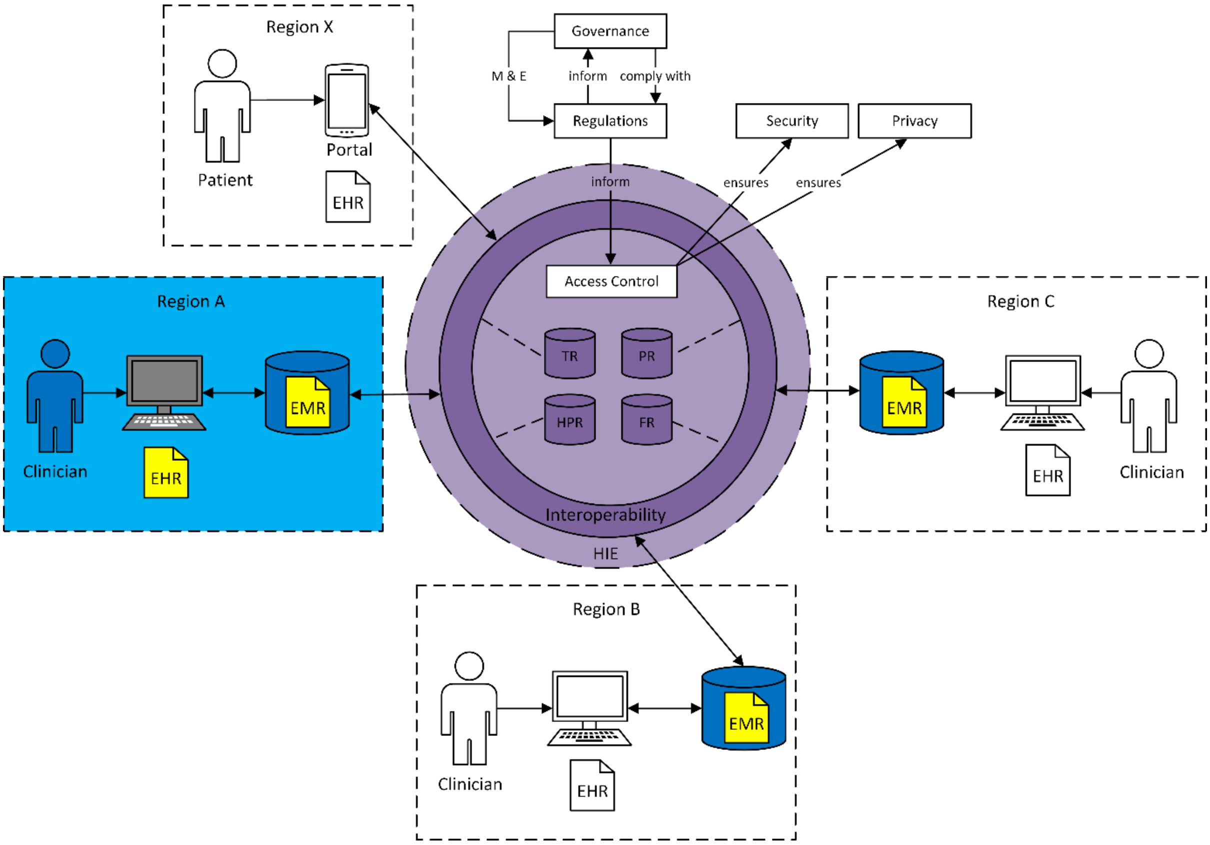


Figure 8.17: Proposed access control model - Interoperability view

EMRs belonging to the same patient. The next section discusses the general systems theory in terms of how it can be applied to the proposed model.

8.7. Application of General Systems Theory to Proposed Model

The operation of the proposed model can be explained by applying the general systems theory to this model. According to von Bertalanffy (as cited in McIntyre, 2016), the general systems theory can be applied to any 'whole' that consists of interacting parts. Applied to the proposed model, the national EHR system is comprised of numerous parts which correspond to regional EMR systems. It is important to note that the operation of the national EHR system would depend on its parts i.e. EMR systems. Thus, an EMR system which is not interoperable would result in the generation of a fragmented EHR which does not contain all the patient's information. Wang and Li (2018) mention a number of key concepts of the general systems theory, which can be applied to the proposed model. With regards to the concept of a hierarchical structure, the overall system i.e. national EHR system can be represented hierarchically in terms of its parts: these parts corresponding to regional EMR systems can be further broken down into the EMRs which they contain. Another important concept of the general systems theory is that all systems must transform inputs into outputs in order to achieve a specific goal. In the proposed model, inputs correspond to the patient's EMRs while the transformation is performed by the central system which aggregates the EMRs of the patient resulting in the output of a national EHR. The output of a national EHR should achieve the goal of improved healthcare. Feedback is also an important concept which will ensure that the system operates more effectively. For instance, feedback in the form of system alerts can indicate if there are any issues when generating the national EHR and can be acted upon in order to address these issues. Lastly, emergence is another key concept of the general systems theory which is applicable to the proposed model. According to Capra and Luisi (as cited in McIntyre, 2016), emergent properties arise when there is an interaction between the parts which together form the whole. In the context of this study, emergence would result in a secure, private and interoperable national EHR system. This chapter is summarised in the next section.

8.8. Summary

In this chapter, the proposed access control model was covered in detail. The study's research problem was revisited in order to show how the proposed model addresses it. The research problem indicated that there is complexity involved in balancing the requirements of security, privacy and access of the EHR and that patients' EHRs are at risk due to the sharing of EHRs with an increasing number of parties. The development of the proposed model was also discussed which indicated that it was informed by the content analysis and expert review. Critical thinking, which also informed the proposed model through an extensive literature review, was discussed. The study's argument diagram, which was the result of critical thinking, was then covered which included a justification of the proposed model's key components. This was followed by a discussion of the proposed model in terms of its components. Access control, which was the central component, was discussed in terms of how it limits access to authorised clinicians while also allowing emergency access. The operation of access control was informed by the study's theoretical foundation which was applied to the proposed model. A TB scenario was also applied to the proposed model which indicated how the proposed model can represent a real-world healthcare scenario. Lastly, the general systems theory was applied to the proposed model, which presented an alternate view on how the proposed model operates. In the next chapter, this research study is concluded.

CHAPTER 9: CONCLUSION

9.1. Introduction

In this chapter, the research study is summarised and concluded. The research problem is revisited as well as the research questions, which includes how each sub-question was answered by the study. The contribution of this study, which is the proposed model, is also discussed along with how the contribution of improvement was made over existing national EHR system architectures. Lastly, the limitations of the study are also covered as well as the future research areas of the study.

9.2. Research Problem

South Africa's aim of establishing a national EHR system is faced with a number of issues with regards to the security and privacy of patient information as well as the interoperability of its health information systems. The EHR is a digital version of the patient's paper-based records which represents the patient's lifetime (Canada Health Infoway, 2006c). As a result of containing health information over the patient's lifetime, the confidentiality of information must be ensured. On the other hand, the EHR should be shared between clinicians in order to treat the patient. Thus, confidentiality cannot be ensured since clinician access to the patient's EHR would violate the patient's confidentiality. Hence, access control is required in order to provide the right level of secure EHR access to authorised clinicians.

In addition, a lack of interoperability between South African health information systems has resulted in a number of disparate systems which cannot communicate with one another (Department of Health South Africa, 2012). As a result, a national EHR system cannot be realised and this will not enable the sharing of EHRs between authorised clinicians. Thus, interoperability is required in order to realise a national EHR system. Access control and interoperability are linked: without interoperability, access control cannot be enforced on a national EHR system.

Thus, the research problem is that there is complexity involved in balancing the requirements of security, privacy and access of the EHR. The security and privacy of patients' EHRs are at risk due to the sharing of the EHRs with an increasing number of parties. This complexity would need to be addressed through the use of access control. Additionally, by addressing interoperability, access control can be enforced on a national EHR system. In the next section, the research questions of the study are addressed.

9.3. Research Questions

The main research question, which is based on the previously discussed research problem, is: **How should access control be enforced to realise a secure and private South African national electronic health record system?** The main research question was answered by addressing the following four sub-questions:

1. **What can South Africa learn from other countries in order to implement a secure national electronic health record system?**

This sub-question focussed on the national EHR implementations of five countries: Canada, New Zealand, South Africa, Sweden and England as well as the challenges that were experienced by these countries during their national EHR implementations, which served as lessons learned for future implementations.

The examined countries' national EHR implementations were discussed which identified the countries that were at an advanced stage as well as those countries which were still at the planning stage with a conceptual national EHR system. This discussion also included the EHR system architectures which indicated the important components of a national EHR system. The proposed model was informed by this discussion and thus included important components such as interoperability, a patient portal and registries. The examined countries' EHR system architectures were based on either the distributed or centralised architecture, which determined how the national EHR would be accessed. Based on the advantages and disadvantages of both the distributed and centralised architectures, the proposed model incorporated the distributed architecture for providing access to the national EHR. Lastly, the challenges that the examined countries faced during their national EHR implementations were covered which served as lessons learned which can assist South Africa's future implementation of a national EHR system. In addition, some of these challenges have been addressed by the proposed model such as security and privacy issues, governance issues and lack of interoperability.

This sub-question assisted with addressing the research problem as it provides insight on a national EHR system architecture that needs to be implemented before access control can be used to secure the national EHR system.

2. **What type of regulations must be followed in order for a compliant national electronic health record system to be achieved?**

This sub-question examined the regulations of the previously mentioned countries: Canada, New Zealand, South Africa, Sweden and England. The examined regulations also included HIPAA, the Data Protection Directive and the GDPR. Additionally, security and privacy standards comprising of ISO/IEC 27001 and ISO/IEC 29100, which aid compliance with regulations, were discussed.

The examined regulations were compared against South Africa's PoPI Act principles which indicated convergence. This indicated that the PoPI Act's principles were aligned to other countries' regulations. In addition, the PoPI Act was also compared to the examined regulations based on the characteristics of regulations such as processing and security. These two comparisons were important to make since the regulation of a South African national EHR system would be influenced by the PoPI Act. Furthermore, two important security and privacy standards were examined: the ISO/IEC 29100 privacy framework and ISO/IEC 27001 information security management system standards, which can be used to aid compliance with regulations. The proposed model was informed by this discussion and incorporated the regulations component, which includes the PoPI Act. In addition, the standards component was included in the proposed model to cover both ISO/IEC 29100 and ISO/IEC 27001. The proposed model also indicated the relationship between regulations, standards and access control.

This sub-question's coverage of regulations assisted with addressing the research problem since access control, which can be used to protect patient information, is informed by regulations. As a result, the rules, which have been defined by regulations such as the PoPI Act, have been used to inform how access control will operate in order to secure the national EHR.

3. **How can access control be used to restrict electronic health record access to authorised clinicians while also logging electronic health record access?**

This sub-question set out to cover how access control can be used to secure the EHR. Access control was discussed in terms of its components: identification, authentication, authorisation and accountability. Also discussed was the ANSI RBAC standards and Clark-Wilson model, which were part of the study's theoretical foundation.

Securing the EHR using access control is important as the realisation of a South African national EHR system would result in patients' EHRs being accessible nationally. In order to secure the EHR, each component of access control was examined. This discussed how the IAAA should be used to identify, authenticate and authorise the clinician by providing the right level of access and audit the actions taken by the clinician when accessing the EHR. Access control and the IAAA components were added to the centre of the proposed model to emphasise the importance of access control. With regards to authentication, two-factor authentication consisting of a smart card and SSO were selected for the proposed model's authentication component. For the proposed model's authorisation component, it was decided that authorisation would be based on a combination of RBAC and ABAC: RBAC for authorising clinicians based on their role while ABAC was used to handle emergencies. These choices were based on ANSI RBAC standards: ANSI INCITS 359-2012 and ANSI INCITS 494-2012 which formed part of the study's theoretical foundation. The Clark-Wilson model also formed part of the study's theoretical foundation and was used to indicate that clinicians would only be able to access the EHR in a constrained manner that would ensure integrity of the EHR.

This sub-question helped with addressing the research problem through the examination of access control. Access control can be used to address the security and privacy aspects of the research problem by limiting EHR access to authorised clinicians while at the same time ensuring that authorised clinicians can only access patient information that they need to know to perform their job function.

4. **What is required to realise an interoperable national electronic health record system?**

This sub-question focussed on interoperability, more specifically healthcare interoperability standards that are required in order to realise an interoperable national EHR system. The three levels of interoperability: foundational, syntactic and semantic interoperability were also covered along with healthcare interoperability standards that can be used to ensure interoperability. The use of the HSB for ensuring interoperability through the implementation of interoperability standards was also covered.

The realisation of an interoperable national EHR system was achieved by examining each of the three levels of interoperability. Since the focus was on healthcare interoperability standards, the discussion of specific standards were limited to the syntactic and semantic levels. Healthcare interoperability standards including HL7 and DICOM standards were discussed for achieving syntactic interoperability. With regards to semantic interoperability, the discussed standards included HL7, LOINC, ICD-10 and SNOMED CT standards for achieving semantic interoperability. The IHE initiative was also discussed in terms of how it can be used to address specific use cases such as 'query laboratory test results' through the use of IHE profiles which identify specific interoperability standards that can be implemented in order to ensure interoperability. The HSB was also examined which indicated how the discussed standards could be implemented to achieve interoperability between disparate systems. This discussion informed the proposed model which included the interoperability layer. The proposed model's interoperability layer was identified as the HSB and was discussed in terms of how it ensures all three levels of interoperability.

This sub-question's focus on interoperability helped address the research problem since a national EHR system cannot be established unless interoperability exists between its subsystems i.e. EMR systems. Additionally, without interoperability, access control would not be enforced on a national EHR system. Thus, the examination of interoperability was an important part of the research problem.

The answers to the above sub-questions informed the development of the proposed model which resulted in an access control model that addressed the security, privacy and interoperability issues that a South African national EHR system would face. The proposed model was the contribution of this study and is covered next.

9.4. Contribution of Study

The proposed model, which serves as the contribution of this study, was discussed in Chapter 8: Section 8.6 in terms of its components which together addressed the research problem (the proposed model is illustrated in Figure 8.4). The development of the proposed model followed the design science research paradigm and was informed by the results of the content analysis and expert review. According to the discussions from the previous section, it is evident that the proposed model was also informed by an extensive literature review which was conducted using critical thought. This resulted in a number of key concepts being incorporated into the proposed model as components, which assisted with addressing the research problem. Also discussed in the previous section was how the proposed model addressed the research problem by answering the four sub-questions. With regards to the operation of access control in the proposed model, this was informed by the ANSI RBAC standards and the Clark-Wilson model, which formed part of the study's theoretical foundation.

The proposed model makes a number of improvements over other national EHR system architectures. Firstly, the IAAA is illustrated and indicates the components of access control that are required in order to control access to the national EHR. The available access control models from the literature do not illustrate the use of the IAAA for securing the national EHR. The proposed model makes an improvement over other national EHR system architectures by illustrating how disparate EMRs are aggregated to form the national EHR. The proposed model also presents the concept of tiered EHRs by indicating how the second tier EHR and first tier EHR are generated with and without the distributed architecture respectively. In addition, the proposed model also represents the relationship between regulations and access control which shows how access control is informed by regulations. This is an important relationship that has not been illustrated in the national EHR system architectures of the countries which were examined in Chapter 3: Section 3.4.3. The limitations of the study are covered next.

9.5. Limitations of Study

This section covers the limitations of the study which included aspects of the national EHR system which were not covered due to the specific scope of the study. This study did not focus on the costs that are involved in the establishment of a national EHR system. In addition to ensuring a secure, private and interoperable national EHR system, costs would need to be addressed since establishing and securing a national EHR system would require funding. While this study discussed how interoperability can be ensured between disparate systems, a limitation is that some systems may not be interoperable such as paper-based systems and some legacy systems, which may still be used by health facilities. The next section covers the future research areas of this study.

9.6. Future Research

Future research can build on two-factor authentication, which was presented in the proposed model, by investigating how the use of all three factors of authentication can be used to secure the EHR while reducing the impact on usability. One of the factors of authentication can include behavioural biometrics, which will allow clinicians that wear clinical gloves to authenticate. Future research can also build on the proposed model's use of the distributed architecture for accessing the national EHR by investigating how blockchain technology can be used to increase the level of security with regards to the EHR. Lastly, a prototype of the proposed model can be developed in order to test how the proposed model would perform in the real world. The research study is summarised in the next section.

9.7. Summary

This chapter served as the concluding chapter of this study and began with revisiting the research problem, which this research study set out to address. The main research question of the study was divided into four sub-questions in order to be answered. Each sub-question corresponded to a literature review chapter which was summarised. Additionally, each sub-question was answered and the manner in which the literature review chapter informed the proposed model was also discussed. This was followed by the discussion of the proposed model, which served as the contribution of this study and has made a number of improvements over other national EHR system architectures. The limitations of the study were then covered. Finally, the future research areas of this study were discussed. The proposed model can be used in the South African context to address the security and privacy which South Africa’s national EHR system would face while also providing EHR access in an emergency.

REFERENCE LIST

Abu-Nimeh, S. (2011). Three-Factor Authentication. In *Encyclopedia of Cryptography and Security* (2nd ed., Vol. 1, pp. 1287-1288). New York, NY: Springer.

Alhaqbani, B., & Fidge, C. (2007). Access Control Requirements for Processing Electronic Health Records. *International Conference on Business Process Management* (pp. 371–382). Brisbane: Springer.

Ali, J. (n.d.). Tuberculosis Education and Information. Retrieved from https://www.medschool.lsuhsc.edu/tb/casestudy01.aspx

Aliakbarpoor, Y., Comai, S., & Pozzi, G. (2017). Designing a HL7 Compatible Personal Health Record for Mobile Devices. *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry* (pp. 1–6). Modena: IEEE.

AlJarullah, A., & El-Masri, S. (2013). A Novel System Architecture for the National Integration of Electronic Health Records: A Semi-Centralized Approach. *Journal of Medical Systems*, 37(4), 1–20.

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Multi Factor Authentication Using Mobile Phones. *International Journal of Mathematics and Computer Science*, 4(2), 65–80.

Alyea, J. M., Dixon, B. E., Bowie, J., & Kanter, A. S. (2016). Standardizing Health-Care Data Across an Enterprise. In B. E. Dixon (Eds.), *Health Information Exchange: Navigating and Managing a Network of Health Information Systems* (pp. 137-148). London: Elsevier.

Angkananon, K., Wald, M., & Gilbert, L. (2013). *Findings of Expert Validation and Review of the Technology Enhanced Interaction Framework*. Unpublished manuscript, Department of Electronics and Computer Science, University of Southampton, Southampton, England.

Australian Cyber Security Centre. (2017). *Multi-factor Authentication*. Retrieved from https://acsc.gov.au/publications/protect/Multi_Factor_Authentication.pdf

Benson, T. (2012). *Principles of Health Interoperability HL7 and SNOMED* (2nd ed.). London: Springer.

Bertino, E., & Takahashi, K. (2011). *Identity Management: Concepts, Technologies, and Systems*. Norwood: Artech House.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law and Security Report*, 24(6), 508–520.

Botha, J., Eloff, M. M., & Swart, I. (2015). Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa. *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 39–48). Reading: Academic Conferences and Publishing International.

Braunstein, M. L. (2018). *Health Informatics on FHIR: How HL7 's New API is Transforming Healthcare*. Cham: Springer.

Breaux, T. D., & Antón, A. I. (2008). Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE Transactions on Software Engineering*, 34(1), 5–20.

Brennan, S. (2007). The biggest computer programme in the world ever! How's it going? *Journal of Information Technology*, 22(3), 202–211.

Brose, G. (2011). Password. In *Encyclopedia of Cryptography and Security* (2nd ed., Vol. 1, pp. 916-918). New York, NY: Springer.

Brown, S. (2018). The "new" PIPEDA data breach notification requirements: Twelve years in the making. Retrieved from https://iapp.org/news/a/the-new-pipeda-data-breach-notification-requirements-twelve-years-in-the-making/

Broyles, D., Dixon, B. E., Crichton, R., Biondich, P., & Grannis, S. J. (2016). The Evolving Health Information Infrastructure. In B. E. Dixon (Eds.), *Health Information Exchange: Navigating and Managing a Network of Health Information Systems* (pp. 107-122). London: Elsevier.

Bunniss, S., & Kelly, D. R. (2010). Research paradigms in medical education research. *Medical Education*, 44(4), 358–366.

Byun, J.-W., Sohn, Y., & Bertino, E. (2006). Systematic Control and Management of Data Integrity. *Proceedings of the 11th ACM symposium on Access control models and technologies* (pp. 101–110). Tahoe City: ACM.

Canada Health Infoway. (2006a). *An overview of the Electronic Health Record Privacy and Security Conceptual Architecture*. Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/388-ehr-privacy-and-security-architecture-summary

Canada Health Infoway. (2006b). *EHRS Blueprint: an interoperable EHR framework - Version 2*. Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/391-ehrs-blueprint-v2-full

Canada Health Infoway. (2006c). *EHRS Blueprint: an interoperable EHR framework - Version 2 (Summary)*. Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/390-ehrs-blueprint-v2-summary?Itemid=101

Cankaya, E.C. (2011a). Bell-LaPadula Confidentiality Model. In Encyclopedia of Cryptography and Security (2nd ed., Vol. 1, pp. 72-74). New York, NY: Springer.

Cankaya, E.C. (2011b). Chinese Wall Model. In *Encyclopedia of Cryptography and Security* (2nd ed., Vol. 1, pp. 203-205). New York, NY: Springer.

Cavalini, L. T., & Cook, T. W. (2015). Semantic interoperability of controlled vocabularies in medicine: A case study of the International Statistical Classification of Diseases 'Tuberculosis' subset. *Computers in Industry*, 69, 30–34.

Chang, F., & Gupta, N. (2015). Progress in electronic medical record adoption in Canada. *Canadian Family Physician*, 61(12), 1076–1084.

Chen, K., Shing, M., Lee, H., & Shing, C. (2007). Modeling in Confidentiality and Integrity for a Supply Chain Network. *Communications of the International Information Management Association*, 7(1), 41–48.

Chuvakin, A., & Peterson, G. (2010). How to Do Application Logging Right. *IEEE Security and Privacy*, 8(4), 82–85.

Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. *1987 IEEE Symposium on Security and Privacy* (pp. 184-194). Oakland: IEEE.

Clarke, G. (2014, September 9). NHS grows a NoSQL backbone and rips out its Oracle Spine. *The Register*. Retrieved from https://www.theregister.co.uk/2014/09/09/nhs_spin2_rips_out_oracle/

Coetzer, C. (2015). *An investigation of ISO/IEC 27001 adoption in South Africa* (Master's thesis, Rhodes University, Grahamstown, South Africa). Retrieved from http://hdl.handle.net/10962/d1018669

Coiera, E. W. (2007). Lessons from the NHS National Programme for IT. *Medical Journal of Australia*, 186(1), 3–4.

Conover, K. (n.d.). EMR vs EHR vs PHR. Retrieved from http://ed-informatics.org/healthcare-it-in-a-nutshell-2/emr-vs-ehr-vs-phr/

Corepoint Health. (n.d.). HL7 ADT–Admit Discharge Transfer. Retrieved from https://corepointhealth.com/resource-center/hl7-resources/hl7-adt/

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks: SAGE.

CSIR & Department of Health. (2014). *National Health Normative Standards Framework for Interoperability in eHealth in South Africa: Version 2.0*. Retrieved from http://www.samed.org.za/Filemanager/userfiles/hnsf-complete-version.pdf

Dallons, G., Massonet, P., Molderez, J. F., Ponsard, C., & Arenas, A. (2007). An Analysis of the Chinese Wall Pattern for Guaranteeing Confidentiality in Grid-based Virtual Organisations. *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks* (pp. 1–6). Nice: IEEE.

Damon, F., & Coetzee, M. (2013). Towards a generic Identity and Access Assurance model by component analysis - a conceptual review. *Proceedings of the 1st International Conference on Enterprise Systems* (pp. 1-11) Cape Town: IEEE.

Data Protection Act (2018). The National Archives (c. 12). United Kingdom.

De Capitani di Vimercati, S., & Samarati, P. (2011). Clark and Wilson Model. In *Encyclopedia of Cryptography and Security* (2nd ed., Vol. 1, pp. 208-209). New York, NY: Springer.

De Lusignan, S., & Seroussi, B. (2013). A comparison of English and French Approaches to Providing Patients Access to Summary Care Records: Scope, Consent, Cost. *Studies in Health Technology and Informatics*, 186, 61–65.

De Soete, M. (2011). Token. In Encyclopedia of Cryptography and Security (2nd ed., Vol. 1, pp. 1305-1306). New York, NY: Springer.

Dekker, M. A. C., & Etalle, S. (2007). Audit-Based Access Control for Electronic Health Records. *Electronic Notes in Theoretical Computer Science*, 168, 221–236.

Deloitte. (2015). *Independent review of New Zealand's Electronic Health Records Strategy*. Retrieved from http://www.health.govt.nz/publication/independent-review-new-zealands-electronic-health-record-strategy

Department of Health England. (2012). *The power of information: Putting all of us in control of the health and care information we need*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf

Department of Health South Africa. (2012). *eHealth Strategy South Africa*. Retrieved from https://www.health-e.org.za/wp-content/uploads/2014/08/South-Africa-eHealth-Strategy-2012-2017.pdf

Desai, P. (2012). *The Break-the-Glass (BtG) principle in Access Control* (Master's thesis, Rochester Institute of Technology, New York, United States). Retrieved from https://www.researchgate.net/profile/Kawade_Rajendra/publication/266888670_The_Break-the-Glass_BtG_principle_in_Access_Control/links/55e971e808ae65b6389af45e.pdf

Directive 95/46/EC (1995). Official Journal of the European Communities (No. L 281/31). European Union.

DLA Piper. (2018). *Data Protection Laws of the World: Full Handbook*. Retrieved from DLA Piper: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all

Dolin, R. H., & Alschuler, L. (2011). Approaching semantic interoperability in Health Level Seven. *Journal of the American Medical Informatics Association*, 18(1), 99–103.

Duncan, B., & Whittington, M. (2016). Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail. *The 7th International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 125–130). Rome: IARIA.

eHealth Ontario. (2017). *Auditing and Monitoring Guide: Electronic Health Record*. Retrieved from https://www.ehealthontario.on.ca/images/uploads/support/Privacy_Toolkit/08_EHR_Auditing_and_Monitoring_Guide_v_1.0.pdf

Eisenberg, S. A. (2001). *Primer on the HIPAA Privacy Regulations.* Retrieved from Employers Resource Association: https://hrxperts.org/pdf/library/hr/143_-_hipaa_privacy_regulations.pdf

Estes, A. (2011). Biba Integrity Model. In *Encyclopedia of Cryptography and Security* (2nd ed., Vol. 1, pp. 81). New York, NY: Springer.

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

Firat, M., & Yurdakul, I. K. (2011). Virtual Ethnography Research on Second Life Virtual Communities. *Turkish Online Journal of Distance Education*, 12(3), 108–117.

Frisse, M. E. (2017). Interoperability. In A. Sheikh, K. M. Cresswell, A. Wright, & D. W. Bates (Eds.)*, Key Advances in Clinical Informatics: Transforming Health Care Through Health Information Technology* (pp. 69-77). London: Elsevier.

Furnell, S. M., Katsikas, S., Lopez, J., & Patel, A. (2008). *Securing Information and Communications Systems: Principles, Technologies, and Applications*. Norwood: Artech House.

Gagnon, M.-P., Payne-Gagnon, J., Breton, E., Fortin, J.-P., Khoury, L., Dolovich, L., … Archer, N. (2016). Adoption of Electronic Personal Health Records in Canada: Perceptions of Stakeholders. *International Journal of Health Policy and Management*, 5(7), 425–433.

General Data Protection Regulation (2016). Council of the European Union (No. 5419/16). European Union.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), 135–146.

Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., & Russell, J. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace. *BMJ*, 341(7782), 1-11.

Gregg, M. (2017). *CISSP Exam Cram* (4th ed.). Pearson Education.

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *Management Information Systems Quarterly, 37*(2), 337–355.

Hammami, R., Bellaaj, H., & Kacem, A. H. (2014). Interoperability for medical information systems: an overview. *Health and Technology*, 4(3), 261–272.

Hägglund, M., & Scandurra, I. (2017). Patients' online access to Electronic Health Records – current status and experiences from the implementation in Sweden. *Proceedings of the 16th World Congress on Medical and Health Informatics* (pp. 723-727). Hangzhou: IOS Press.

Heckle, R. R., & Lutters, W. G. (2011). Tensions of network security and collaborative work practice: Understanding a single sign-on deployment in a regional hospital. *International Journal of Medical Informatics*, 80(8), e49–e61.

Helms, E., & Williams, L. (2011). Evaluating Access Control of Open Source Electronic Health Record Systems. *Proceedings of the 3rd Workshop on Software Engineering in Health Care* (pp. 63-70). Honolulu: ACM.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly, 28*(1), 75–105.

Heymans, S., McKennirey, M., & Phillips, J. (2011). Semantic validation of the use of SNOMED CT in HL7 clinical documents. *Journal of Biomedical Semantics*, 2(2), 1–16.

Hoepman, J.-H. (2013). *Privacy Design Strategies*. Unpublished manuscript, Institute for Computing and Information Sciences, Radboud University, Nijmegen, Netherlands.

Hosseini, M., & Dixon, B. E. (2016). Syntactic Interoperability and the Role of Standards. In B. E. Dixon (Eds.), *Health Information Exchange: Navigating and Managing a Network of Health Information Systems* (pp. 123-136). London: Elsevier.

House of Commons. (2007). *Department of Health: The National Programme for IT in the NHS - Twentieth Report of Session 2006-07*. Retrieved from https://publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/390/390.pdf

Huang, Y., Huang, Z., Zhao, H., & Lai, X. (2013). A new One-time Password Method. *IERI Procedia*, 4, 32–37.

INCITS. (2012a). *INCITS 359-2012 Information Technology - Role Based Access Control*. New York: ANSI.

INCITS. (2012b). *INCITS 494 Information Technology - Role Based Access Control - Policy-Enhanced*. New York: ANSI.

Information Commissioner’s Office. (2018). *The Guide to Data Protection*. Retrieved from http://www.ico.org.uk/for_organisations/guide_to_data_protection

Iroju, O., Soriyan, A., Gambo, I., & Olaleke, J. (2013). Interoperability in Healthcare: Benefits, Challenges and Resolutions. *International Journal of Innovation and Applied Studies*, 3(1), 262–270.

ISO/IEC. (2011). *ISO/IEC 29100 - Information technology - Security techniques - Privacy framework*. Geneva: ISO/IEC.

ISO/IEC. (2013). *ISO/IEC 27001:2013 - Information technology - Security techniques - Information security - management systems - Requirements*. Geneva: ISO/IEC.

Jalal-Karim, A., & Balachandran, W. (2008). The optimal network model’s performance for sharing Electronic Health Record. *2008 IEEE International Multitopic Conference* (pp. 149–154). Karachi: IEEE.

Janols, R., Lind, T., Göransson, B., & Sandblad, B. (2014). Evaluation of user adoption during three module deployments of region-wide electronic patient record systems. *International Journal of Medical Informatics*, 83(6), 438–449.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research*, 1(2), 112–133.

Khan, A. R. (2012). Access Control in Cloud Computing Environment. *Asian Research Publishing Network Journal of Engineering and Applied Sciences*, *7*(5), 613–615.

Kierkegaard, P. (2011). Electronic health record: Wiring Europe’s healthcare. *Computer Law and Security Review*, 27(5), 503–515.

Kozlov, R. (2014). *Case Study: Diagnosis and Treatment of Mycobacterium tuberculosis*. Retrieved from Test Target Treat: https://www.testtargettreat.com/en/home/educational-resources/case-studies/tuberculosis-case-study.html

Krippendorff, K. (2013). *Content Analysis: An Introduction to Its Methodology* (3rd ed.). Thousand Oaks: SAGE.

Kubicek, H., Cimander, R., & Scholl, H. J. (2011). *Organizational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases*. Berlin: Springer.

Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding Attributes to Role-Based Access Control. *IEEE Computer*, 43(6), 79–81.

Kumar, A. (2013, May). *Security Analysis of Web-based Identity Federation*. Paper presented at Web 2.0 Security & Privacy 2013, San Francisco.

Kush, R. D. (2012). *Data Sharing: Electronic Health Records and Research Interoperability*. London: Springer.

Law Commission. (2010). *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*. Retrieved from http://www.lawcom.govt.nz/UploadFiles/Publications/Publication_129_460_Whole Document.pdf

Macia, I. (2014). Towards a Semantic Interoperability Environment. *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 543–548). Natal: IEEE.

Mao, Z., Li, N., Chen, H., & Jiang, X. (2009). Trojan Horse Resistant Discretionary Access Control. *Proceedings of the 14th ACM symposium on Access control models and technologies* (pp. 237–246). Stresa: ACM.

McIntyre, P. (2016). General Systems Theory and Creativity. In McIntyre, P., Fulton, J., & Paton, E. (Eds.). *The Creative System in Action: Understanding Cultural Production and Practice* (pp. 13-26). Basingstoke, England: Palgrave Macmillan.

Ministry of Health and Social Affairs. (2010). *National eHealth - the strategy for accessible and secure information in health and social care*. Retrieved from http://www.government.se/reports/2011/05/national-ehealth---the-strategy-for-accessible-and-secure-information-in-health-and-social-care/

Ministry of Justice. (2006). *Personal Data Protection: Information on the Personal Data Act*. Retrieved from https://www.government.se/information-material/2006/12/personal-data-protection/

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Public Library of Science Medicine*, 6(7), 1–6.

Mustafić, T., Messerman, A., Camtepe, S. A., Schmidt, A.-D., & Albayrak, S. (2011). Behavioral Biometrics for Persistent Single Sign-on. *Proceedings of the 7th ACM workshop on Digital identity management* (pp. 73-82). Chicago: ACM.

NetIQ. (2016). *Hard Tokens vs. Soft Tokens: Why Soft Tokens Area the Better Option.* Retrieved from https://www.netiq.com/docrep/documents/xvbozdzzxj/hard_tokens_vs_soft_tokens_fpp.pdf

Nguyen, D. (2015). Soft vs Hard Tokens. Retrieved from https://hypersecu.com/blog/90-soft-vs-hard-tokens

Nieuwesteeg, B. (2016). Quantifying Key Characteristics of 71 Data Protection Laws. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 7(3), 182-203.

Office of the Privacy Commissioner of Canada. (2015). *Privacy Toolkit: A Guide for Businesses and Organizations*. Retrieved from https://www.priv.gc.ca/media/2038/guide_org_e.pdf

Ohuabunwa, E. C., Sun, J., Jean Jubanyik, K., & Wallis, L. A. (2016). Electronic Medical Records in low to middle income countries: The case of Khayelitsha Hospital, South Africa. *African Journal of Emergency Medicine,* 6(1), 38–43.

Olivier, M. S. (2009). *Information Technology Research: A practical guide for Computer Science and Informatics* (3rd ed.). Pretoria: Van Schaik.

Öberg, U., Orre, C. J., Isaksson, U., Schimmer, R., Larsson, H., & Hörnsten, Å. (2018). Swedish primary healthcare nurses' perceptions of using digital eHealth services in support of patient self-management. *Scandinavian Journal of Caring Sciences*, 32(2), 961–970.

Parkin, E. (2016). *A paperless NHS: electronic health records*. Retrieved from http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7572

Parliamentary Office of Science and Technology. (2016). *Electronic Health Records*. Retrieved from http://researchbriefings.files.parliament.uk/documents/POST-PN-0519/POST-PN-0519.pdf

Peekhaus, W. (2008). Personal health information in Canada: A comparison of citizen expectations and legislation. *Government Information Quarterly*, 25(4), 669-698.

Pianykh, O. S. (2012). *Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide* (2nd ed.). Berlin: Springer.

Preuveneers, D., & Joosen, W. (2014). Federated Privileged Identity Management for Break-the-Glass: A Case Study with OpenAM. *Proceedings of the 2nd European Workshop on Practical Aspects of Health Informatics* (pp. 37–52). Trondheim: CEUR Workshop Proceedings.

Protection of Personal Information Act (2013). South African Government Gazette. (Vol. 581, No. 37067). South Africa.

Privacy Act (1993). Parliamentary Counsel Office (No. 28). New Zealand.

Radha, V., & Reddy, D. H. (2012). A Survey on Single Sign-On Techniques. *Procedia Technology*, 4, 134–139.

Rainbolt, G. W., & Dwyer, S. L. (2012). *Critical Thinking: The Art of Argument*. Wadsworth: Cengage Learning.

Rasiwasia, A. (2017). *A Framework To Implement OpenID Connect Protocol For Federated Identity Management In Enterprises* (Master's thesis, Luleå University of Technology, Luleå, Sweden). Retrieved from http://www.diva-portal.org/smash/get/diva2:1121361/FULLTEXT01.pdf

Rayes, M.O. (2011). One-Time-Password. In Encyclopedia of Cryptography and Security (2nd ed., Vol. 1, pp. 885-887). New York, NY: Springer.

Reid, C., & Osborne, G. (2016). *Strategic Assessment: Establishing the Electronic Health Record*. Retrieved from https://www.health.govt.nz/system/files/documents/pages/electronic-health-record-strategic-assessment.pdf

Rexhepi, H., Ahlfeldt, R.-M., & Persson, A. (2015). Challenges and opportunities with information system support for healthcare processes – A healthcare practitioner perspective. *Proceedings of the 8th IADIS International Conference Information Systems* (pp. 61-69). Madeira: IADIS Press.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). *Review of EU Data Protection Directive : Summary.* Retrieved from https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf

Ryan, A., & Eklund, P. (2010). The Health Service Bus: An Architecture and Case Study in Achieving Interoperability in Healthcare. *Studies in Health Technology and Informatics,* 160, 922–926.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). Harlow: Pearson Education.

Schinagl, S., Paans, R., & Schoon, K. (2016). The Revival of Ancient Information Security Models, Insight in Risks and Selection of Measures. *2016 49th Hawaii International Conference on System Sciences* (pp. 4041–4050). Koloa: IEEE.

Sellberg, N., & Eltes, J. (2017). The Swedish Patient Portal and Its Relation to the National Reference Architecture and the Overall eHealth Infrastructure. In M. Aanestad, M. Grisot, O. Hanseth, & P. Vassilakopoulou (Eds.), *Information Infrastructures within European Health Care* (pp. 225–244). Cham, Switzerland: Springer.

Schreier, M. (2012). *Qualitative Content Analysis in Practice*. London: SAGE.

Shamoo, A. E., & Resnik, D. B. (2015). *Responsible Conduct of Research* (3rd ed.). New York: Oxford University Press.

Sifou, F., Hammouch, A., & Kartit, A. (2017). Ensuring Security in Cloud Computing Using Access Control: A Survey. *Proceedings of the Mediterranean Symposium on Smart City Applications* (pp. 255–264). Cham: Springer.

Sittig, D. F. (2017). Audit Logs. *Medical Liability and Health Care Law Seminar* (pp. 1–11). Las Vegas: Defense Research Institute.

Strasbourg, D. (2016). *Electronic Medical Records (EMR) Progress in Canada*. Retrieved from Canada Health Infoway: https://www.infoway-inforoute.ca/en/component/edocman/2860-2016-electronic-medical-records-emr-progress-in-canada/view-document

Svensson, A. F., & Advokatbyrå, H. (2018). *Data protection in Sweden: overview*. Retrieved from https://uk.practicallaw.thomsonreuters.com/8-502-0348

Takian, A., & Cornford, T. (2012). NHS information: Revolution or evolution? *Health Policy and Technology*, 1(4), 193–198.

Terry, N. (2017). Existential challenges for healthcare data protection in the United States. *Ethics, Medicine and Public Health*, 3(1), 19–27.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 34(1), 134–153.

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward Proper Authentication Methods in Electronic Medical Record Access Compliant to HIPAA and C.I.A. Triangle. *Journal of Medical Systems*, *40*(4), 1–8.

Tsang, E. W. K. (2014). Case studies and generalization in information systems research: A critical realist perspective. *Journal of Strategic Information Systems*, 23(2), 174–186.

Tsegaye, T., & Flowerday, S. (2014). Defending Critical Information Infrastructure from Cyberattacks through the Use of Security Controls in Layers. *International Journal for Information Security Research*, 4(4), 490–500.

Vacca, J. (2014). *Managing Information Security* (2nd ed.). Waltham: Syngress.

Vaishnavi, V. K., & Kuechler, W. (2015). *Design Science Research Methods and Patterns* (2nd ed.). Boca Raton: CRC Press.

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, 10(1), 69–80.

Walker, M (2011). *Critical Thinking By Example*. Retrieved from http://www.criticalthinkingbyexample.com/Thecompletebook/1.1%20CTBE%20Book%20June%202011.pdf

Wang, H., & Li, S. (2018). *Introduction to Social Systems Engineering*. Singapore: Springer.

Weber, R. (2012). Evaluating and Developing Theories in the Information Systems Discipline. *Journal of the Association for Information Systems*, 13(1), 1–30.

Weeks, R. (2014). The implementation of an electronic patient healthcare record system: a South African case study. *Journal of Contemporary Management*, 11(1), 101–119.

Wells, S. (2017). The journey of patient portals in New Zealand general practice: early learnings and key challenges. *Journal of Primary Health Care*, 9(4), 237–239.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security* (5th ed.). Boston: Cengage Learning.

Wickramage, C., Sahama, T., & Fidge, C. (2016). Anatomy of Log Files: Implications for Information Accountability Measures. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-6). Munich: IEEE.

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. New York: Springer.

Wu, R., Ahn, G., Hu, H., & Singhal, M. (2010). Information Flow Control in Cloud Computing. *6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010)* (pp. 1–7). Chicago: IEEE.

Yilmaz, K. (2013). Comparison of Quantitative and Qualitative Research Traditions: epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2). 311-325.

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, 1–13.

Zuniga, A. E. F., Win, K. T., & Susilo, W. (2010). Biometrics for Electronic Health Records. *Journal of Medical Systems*, 34(5), 975–983.

APPENDIX A: EXPERT REVIEW QUESTIONNAIRES

Expert Review Questionnaire (Access Control)

Research title: An Access Control Model for a South African National Electronic Health Record System

Research student: Tamir Tsegaye

Supervisor: Prof Stephen Flowerday

Co-supervisor: Prof Graham Wright

*Required

1. **Voluntary consent:** * *Tick all that apply.*

   □ I hereby voluntarily consent to participate in this research.

2. **Is the research problem of balancing the requirements of security, privacy and access of the Electronic Health Record (EHR) relevant?** *Mark only one oval.*

   ○ Yes

   ○ No

3. **Do you think that the proposed model addresses the research problem mentioned in the presentation slides?** *Mark only one oval.*

   ○ Yes

   ○ No

4. **Does the proposed model effectively indicate how it will ensure a secure and private South African national EHR system?** *Mark only one oval.*

   ○ Yes

   ○ No

5. **Is the importance of the proposed model evident through the representation of its focal phenomena i.e. access control?** *Mark only one oval.*

   ○ Yes

   ○ No

6. **Do you think that the proposed model is novel in terms of how it uses access control's IAAA (Identification, Authentication, Authorisation and Accountability) to secure a national EHR system?**

   Mark only one oval.

○ Yes

○ No

7. **Is the relationship between regulations and access control effectively represented by the proposed model?**

Mark only one oval.

○ Yes

○ No

8. **With regards to the number of components used in the proposed model, is this number adequate and not excessive?** *Mark only one oval.*

○ Yes

○ No

9. **Does the proposed model cover its phenomena in a broad or specific way?** *Mark only one oval.*

○ The proposed model's phenomena are covered in a broad way

○ The proposed model's phenomena are covered in a specific way

10. **Could the proposed model be tested in terms of falsifiability?** *Mark only one oval.*

○ Yes

○ No

11. **Is the study's theoretical foundation relevant for securing a national EHR system?** *Mark only one oval.*

○ Yes

○ No

12. **What is your view of the proposed model in terms of how it indicates that clinician/patient access will be controlled using access control's IAAA: Identification, Authentication, Authorisation and Accountability?**

____

____

____

____

____

13. **Do you have any other comments or recommendations regarding the proposed model?**

Expert Review Questionnaire (Health Information Systems)

Research title: An Access Control Model for a South African National Electronic Health Record System
Research student: Tamir Tsegaye
Supervisor: Prof Stephen Flowerday
Co-supervisor: Prof Graham Wright

*Required

1. **Voluntary consent:** * *Tick all that apply.*

   □ I hereby voluntarily consent to participate in this research.

2. **Is the research problem of balancing the requirements of security, privacy and access of the Electronic Health Record (EHR) relevant?** *Mark only one oval.*

   ○ Yes
   ○ No

3. **Do you think that the proposed model addresses the research problem mentioned in the presentation slides?** *Mark only one oval.*

   ○ Yes
   ○ No

4. **Is the importance of the proposed model evident through the representation of its focal phenomena i.e. access control?** *Mark only one oval.*

   ○ Yes
   ○ No

5. **Do you think that the proposed model could be applied to a national EHR system for another country other than South Africa?** *Mark only one oval.*

   ○ Yes
   ○ No

6. **Does the proposed model effectively indicate how interoperability will be ensured in the national EHR system?** *Mark only one oval.*

○ Yes

○ No

7. **With regards to the number of components used in the proposed model, is this number adequate and not excessive?** *Mark only one oval.*

○ Yes No

○

8. **Does the proposed model cover its phenomena in a broad or specific way?** *Mark only one oval.*

○ The proposed model's phenomena are covered in a broad way

○ The proposed model's phenomena are covered in a specific way

9. **Could the proposed model be tested in terms of falsifiability?** *Mark only one oval.*

○ Yes

○ No

10. **What do you think of the proposed model’s use of the distributed architecture for enabling access to a national EHR?**

11. **Do you have any other comments or recommendations regarding the proposed model?**

APPENDIX B: CONTENT ANALYSIS SAMPLE

No	Paper title	Author(s)
1	A development framework for semantically interoperable health information systems	Lopez and Blobel (2009)
2	A model driven approach for the German health telematics architectural framework and security infrastructure	Blobel and Pharow (2007)
3	A study of user requests regarding the fully electronic health record system at Seoul National University Bundang Hospital - Challenges for future electronic health record systems	Yoo et al. (2013)
4	Audit-Based Access Control for Electronic Health Records	Dekker and Etalle (2007)
5	Comparing approaches for advanced e-health security infrastructures	Blobel (2007)
6	Electronic health record: Wiring Europe's healthcare	Kierkegaard (2011)
7	Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments	Ben-Assuli (2015)
8	Implementing security in a distributed web-based EHCR	Sucurovic (2007)
9	Information Governance in NHS's NPfIT: A Case for Policy Specification	Becker (2007)
10	Internet of Things and Smart Objects for M-health Monitoring and Control	Santos, Macedo, Costa, and Nicolau (2014)
11	Inter-organizational future proof EHR systems - A review of the security and privacy related issues	van der Linden, Kalra, Hasman, and Talmon (2009)
12	Learning relational policies from electronic health record access logs	Malin, Nyemba, and Paulett (2011)

13	National efforts to improve health information system safety in Canada, the United States of America and England	Kushniruk, Bates, Bainbridge, Househ, and Borycki (2013)
14	Organizational factors affecting successful adoption of innovative eHealth services: A case study employing the FITT framework	Tsiknakis and Kouroubali (2009)
15	Publishing data from electronic health records while preserving privacy: A survey of algorithms	Gkoulalas-Divanis, Loukides, and Sun (2014)
16	Security and privacy in electronic health records: A systematic literature review	Fernández-Alemán et al. (2013)
17	Situation-Based Access Control: Privacy management via modeling of patient data access scenarios	Peleg, Beimel, Dori, and Denekamp (2008)
18	The EHR-ARCHE project: Satisfying clinical information needs in a Shared Electronic Health Record System based on IHE XDS and Archetypes	Duftschmid et al. (2013)
19	The need to know the history of the use of digital patient data, in particular the EHR	Bakker (2007)
20	Towards Intelligent Personal Health Record Systems: Review, Criteria and Extensions	Genitsaridi, Kondylakis, Koumakis, Marias, and Tsiknakis (2013)
21	User-driven prioritization of features for a prospective InterPersonal Health Record: perceptions from the Italian context	Cabitza, De Michelis, and Simone (2015)
22	Using electronic health records for clinical research: The case of the EHR4CR project	De Moor et al. (2015)
23	Using OWL and SWRL to represent and reason with situation-based access control policies	Beimel and Peleg (2011)
24	Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients	Bourgeois, Taylor, Emans, Nigrin, and Mandl (2008)

APPENDIX C: CODE FOR SCREENING PAPERS OF SYSTEMATIC LITERATURE REVIEW

```
# Python code for retrieving titles of first 25 papers appearing in both
# Google Scholar and ScienceDirect databases.
# Retrieved paper titles to be used as content analysis sample.
# Internet connection required.

from selenium import webdriver
from selenium.webdriver.support.ui import Select
from selenium.common.exceptions import WebDriverException
from selenium.common.exceptions import NoSuchElementException
import sys

def getPapers(browser, science_direct_results):

    global MAX_PAPERS
    global count
    global papers

    # get all links on page (including those with paper titles to be extracted)
    links = browser.find_elements_by_xpath("//a[@href]")

    for link in links:

        txt = link.text
        lnk = link.get_attribute('href')

        # store Next link for accessing next page of results
        if txt == "Next":
            next_page = lnk

        # only search for papers which originate from ScienceDirect
        if "http://www.sciencedirect.com" in lnk and "[HTML]" not in txt:

            # add paper appearing in both ScienceDirect and Google Scholar
            if lnk in science_direct_results:
                papers.append(txt.encode('ascii', 'xmlcharrefreplace'))
                count += 1

        if count == MAX_PAPERS:
            papers.sort()
           # number papers from 1-25
            papers = [str(index + 1) + ". " + paper for index,paper in enumerate(papers)]
            return

    return next_page

# first 25 papers to search for appearing in both databases
MAX_PAPERS = 25

# used to track number of papers
count = 0

papers = []

try:
    # create a new Chrome session
    browser = webdriver.Chrome(executable_path = 'chromedriver.exe')

    browser.implicitly_wait(10)
    browser.maximize_window()

    print('Running...' + '\n')

    # navigate to ScienceDirect
    browser.get("http://www.sciencedirect.com/science/search")

    # fill in necessary search parameters
    browser.find_element_by_name("SearchText").send_keys('"access control"')
    browser.find_element_by_name("addSearchText").send_keys('"electronic health record"')
    # uncheck Books checkbox (only Journals checkbox must be selected)
    browser.find_element_by_id("books").click()
    # select specific date range radio button
    browser.find_element_by_id("dateSelectRadio").click()
    # select date range from 2007
    select = Select(browser.find_element_by_name("fromDate"))
    select.select_by_value("2007")

    select = Select(browser.find_element_by_name("toDate"))

    # if first entry of dropdown is Present, current year is 2017, select Present
    if select.options[0].text == "Present":
        select.select_by_value("Present")

    else:
        # current year is not 2017, select 2017
        select.select_by_value("2017")

    # execute search
    browser.find_element_by_name("RegularSearch").click()

    # display all (200) search results on one page
    select = Select(browser.find_element_by_id("resultsPerPage"))
    select.select_by_value("200")

    science_direct_results = browser.page_source

    # navigate to Google Scholar in new tab
    browser.execute_script('window.open("");')
    browser.switch_to.window(browser.window_handles[-1])
    browser.get("https://scholar.google.co.za/")

    # select Google Scholar advanced search
    browser.find_element_by_id("gs_hdr_arr").click()

    # fill in necessary search parameters
    browser.find_element_by_name("as_q").send_keys('"access control" "electronic health
    record"')
    # filter papers by publisher Elsevier (ScienceDirect)
    browser.find_element_by_name("as_publication").send_keys("Elsevier")
    browser.find_element_by_name("as_ylo").send_keys("2007")
    browser.find_element_by_name("as_yhi").send_keys("2017")

    # execute search
    searchBtn = browser.find_element_by_xpath("//button[contains(@type, 'submit') and
    contains(@name, 'btnG') and not(@id)]")
    searchBtn.click()

    while True:
        next_page = getPapers(browser, science_direct_results)

        if count == MAX_PAPERS:

            print("First 25 papers appearing in both ScienceDirect and Google Scholar")
            print("------------------------------------------------------------------------")

            for paper in papers:
                print paper + "\n"

            sys.exit(0)

        # go to next page of results
        browser.get(next_page)

except NoSuchElementException:
    print("Unable to locate element (internet connection required)")
    sys.exit(1)

except WebDriverException:
    print("chromedriver.exe must be in same directory as generate_sample.py")
    sys.exit(1)

except Exception as e:
    print str(e)
    sys.exit(1)
```

Setup instructions (Windows):

- Download and install Python: https://www.python.org/ftp/python/2.7.13/python-2.7.13.msi. At the 'Customize Python' setup screen, enable 'Add python.exe to Path'.
- Download and install Google Chrome Web Browser: https://www.google.com/chrome/browser/desktop/index.html
- Open the command prompt as Administrator and run the below command to install the selenium library:
    - **pip install selenium**
- Inside the command prompt, change the current working directory to the location of the screen_papers.py script:
    - **cd appendix_c**
- Run the below script to generate the first 25 papers appearing in both Google Scholar and ScienceDirect which will be displayed in the command prompt window:
    - **python screen_papers.py**
- **Notes**:
    - chromedriver.exe must be located in the same directory as screen_papers.py.
    - Paper titles generated by the screen_papers.py script may vary slightly compared to the content analysis sample displayed in Appendix B due to paper search rankings changing over time.
    - The screen_papers.py script was run on the **28 May 2017**. Any user interface changes to the Google Scholar or ScienceDirect search pages, after this date, will affect the functioning of the script.

APPENDIX D: CODE FOR CREATING WORD CLOUD FROM CONTENT ANALYSIS RESULTS

```python
# Python code for creating wordcloud using code frequencies from content analysis results
# using code_frequencies.csv as datasource.

import csv
from wordcloud import WordCloud
import matplotlib.pyplot as plt
import errno
import sys

data = {}

try:
    # read codes and frequencies from code_frequencies.csv file
    with open('datasource/code_frequencies.csv', 'rb') as f:
        reader = csv.reader(f, delimiter=';')

        for code,freq in reader:
            data[code] = float(freq)

    # Generate word cloud image
    wordcloud = WordCloud(width=1600, height=800).generate_from_frequencies(data)

    # Display word cloud image
    plt.figure( figsize=(16,8), facecolor='k')
    plt.imshow(wordcloud, interpolation='bilinear')
    plt.axis("off")
    plt.tight_layout(pad=0)
    plt.show()

except IOError as e:
    if e.errno == errno.ENOENT:
        print("code_frequencies.csv must be placed in same directory as codes2wordcloud.py")
        sys.exit(1)

except ValueError:
    print("code_frequencies.csv not in correct format")
    sys.exit(1)

except Exception as e:
    print str(e)
    sys.exit(1)
```

Setup instructions (Windows):

- Download and install Python: https://www.python.org/ftp/python/2.7.13/python-2.7.13.msi. At the ‘Customize Python’ setup screen, enable ‘Add python.exe to Path’.
- Download and install Microsoft Visual C++ Compiler for Python 2.7: https://download.microsoft.com/download/7/9/6/796EF2E4-801B-4FC4-AB28-B59FBF6D907B/VCForPython27.msi
- Open the command prompt as Administrator and run the below command to install the wordcloud library and matplotlib dependency:
    - **pip install wordcloud**
    - **pip install matplotlib**

- Inside the command prompt, change the current working directory to the location of the codes2wordcloud.py script:
    - **cd appendix_d**
- Run the below script to generate the wordcloud:
    - **python codes2wordcloud.py**
- **Notes**:
    - code_frequencies.csv must be located in the same directory as the codes2wordcloud.py script.
    - code_frequencies.csv contains codes and corresponding frequencies separated by a semi-colon.

APPENDIX E: TUBERCULOSIS SCENARIO

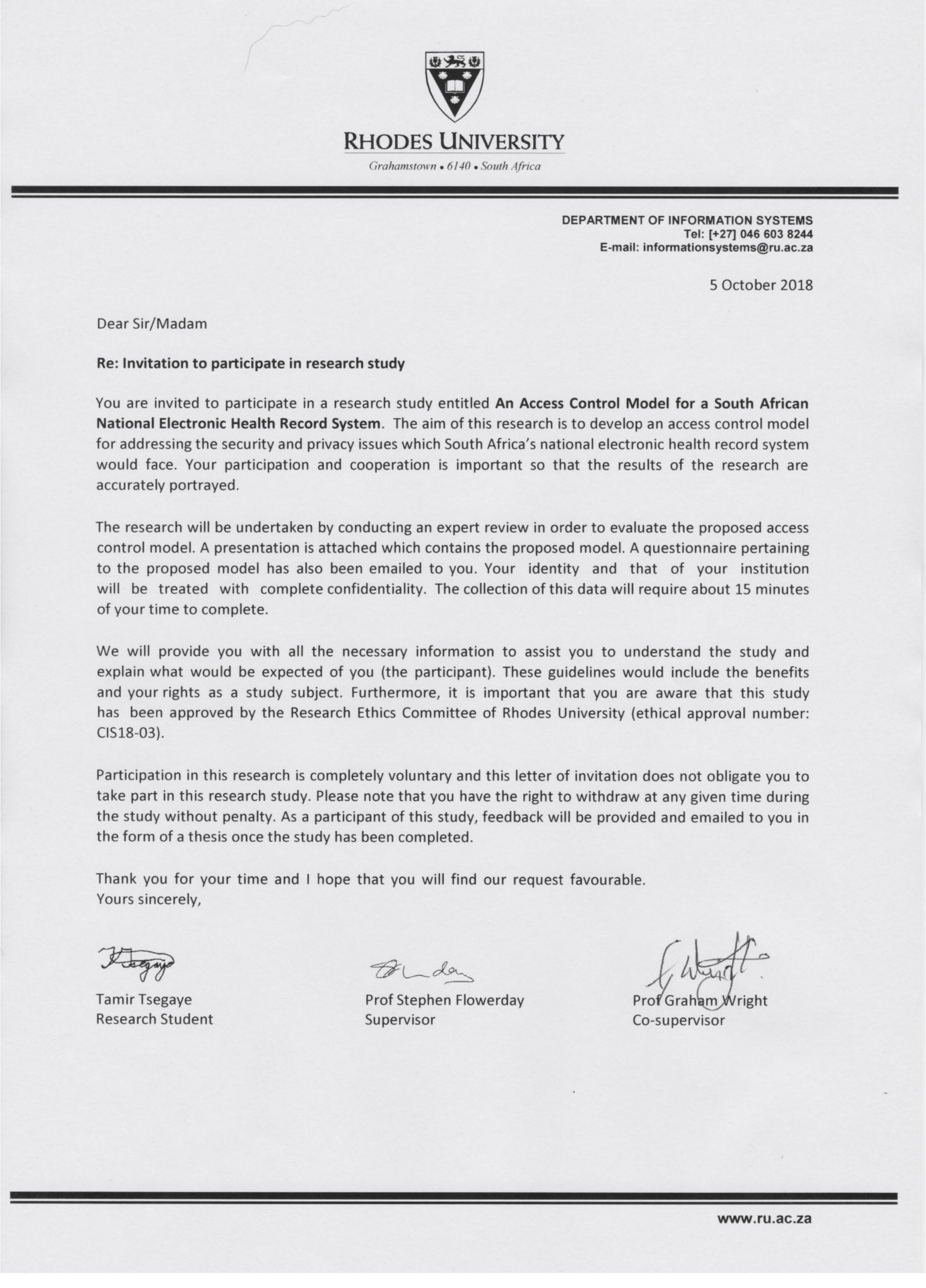
The below TB scenario has been adapted from two TB case studies (Ali, n.d.; Kozlov, 2014):

1. Patient A is not feeling well and has been experiencing symptoms including a persistent cough and shortness of breath.
2. Patient A visits the local clinic.
3. Physician A attends to Patient A and retrieves the patient's EHR in order to view their medical history.
4. Physician A performs an observation of the patient and records it in the patient's EHR.
5. Physician A refers the patient to Radiologist A for a chest X-ray and records this in the patient's EHR.
6. Radiologist A retrieves the patient's EHR in order to view the requested chest X-ray from Physician A.
7. Radiologist A performs the chest X-ray on Patient A and records the results in the patient's EHR.
8. Physician A retrieves the patient's EHR in order to view the result of the chest X-ray.
9. Physician A finds that Patient A's lungs contain signs of cavities.
10. Physician A sends the patient for a further tests.
11. Pathologist A analyses Patient A's test results and records the results in the patient's EHR.
12. After a few days, Patient A returns to the clinic to find out their test results.
13. Physician A views the patient's EHR and informs them that they have contracted TB.
14. Physician A prescribes medication for the patient and records it in the patient's EHR.
15. Patient A goes to the pharmacy to collect their medication.
16. Pharmacist A retrieves the patient's EHR to view their prescription.
17. Pharmacist A gives the patient their medication and records this in the patient's EHR.
18. After a few months since being diagnosed with TB, Patient A, who is unconscious, is transported to the emergency department.
19. Physician B, who is working in the emergency department, does not have access to the patient's EHR.
20. Since this is an emergency, Physician B gains access to the patient's EHR by using the break-glass feature.
21. Physician B retrieves the patient's EHR to view the patient's medical history.
22. Physician B performs an observation of the patient and appends it to the patient's EHR.

23. Physician B transfers the patient to be admitted in the local hospital.

24. Nurse A checks and records the patient’s vital signs in the patient’s EHR.

APPENDIX F: EXPERT REVIEW PARTICIPATION LETTER



RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

DEPARTMENT OF INFORMATION SYSTEMS
Tel: [+27] 046 603 8244
E-mail: informationsystems@ru.ac.za

5 October 2018

Dear Sir/Madam

Re: Invitation to participate in research study

You are invited to participate in a research study entitled **An Access Control Model for a South African National Electronic Health Record System**. The aim of this research is to develop an access control model for addressing the security and privacy issues which South Africa's national electronic health record system would face. Your participation and cooperation is important so that the results of the research are accurately portrayed.

The research will be undertaken by conducting an expert review in order to evaluate the proposed access control model. A presentation is attached which contains the proposed model. A questionnaire pertaining to the proposed model has also been emailed to you. Your identity and that of your institution will be treated with complete confidentiality. The collection of this data will require about 15 minutes of your time to complete.

We will provide you with all the necessary information to assist you to understand the study and explain what would be expected of you (the participant). These guidelines would include the benefits and your rights as a study subject. Furthermore, it is important that you are aware that this study has been approved by the Research Ethics Committee of Rhodes University (ethical approval number: CIS18-03).

Participation in this research is completely voluntary and this letter of invitation does not obligate you to take part in this research study. Please note that you have the right to withdraw at any given time during the study without penalty. As a participant of this study, feedback will be provided and emailed to you in the form of a thesis once the study has been completed.

Thank you for your time and I hope that you will find our request favourable.
Yours sincerely,

Tamir Tsegaye
Research Student

Prof Stephen Flowerday
Supervisor

Prof Graham Wright
Co-supervisor

www.ru.ac.za