Informed e-Consent Framework for Privacy Preservation in South African Health Information Systems

by

Lelethu Zazaza

Submitted in fulfilment of the requirements for the degree
Magister Scientiae (Computer Science)
in the Faculty of Engineering, Built Environment and Information Technology
University of Pretoria, Pretoria

June 2020

Publication data:

Lelethu Zazaza. Informed e-Consent Framework for Privacy Preservation in South African Health Information Systems. Master's dissertation, University of Pretoria, Department of Computer Science, Pretoria, South Africa, June 2020.

Informed e-Consent Framework for Privacy Preservation in South African Health Information Systems

by

Lelethu Zazaza

Abstract

The South African Constitution advocates the protection of personal information. Everyone has the right to privacy. This includes the protection of special information that relates to an individual's biometrics, health, religion, or sex life, to name a few. This special information may be processed if it is necessary in law; if it is being processed for historical purposes; or if it has already been disseminated in public by the data subject. If the aforementioned conditions are not met, the processing of special information is prohibited, unless the data subject has provided consent.

Given that health information is regarded as special information, consent must be obtained from the data subject before it is processed. If the special information is accessed by unauthorised parties it may influence decisions about the data subject's employment, access to credit, and education, and may even cause reputational or personal harm.

This research proposes an e-consent management approach which preserves the privacy of health information. The utilisation of privacy laws and guidelines such as, but not limited to, the Protection of Personal Information Act and the General Data Protection Regulation are used to develop a privacy preserving e-consent model, architectural design and prototype.

The consent obtained from the data subject should be informed and voluntary. In addition, the subject should remain an active participant throughout the processing of his/her personal information. The e-consent management approach developed by the research is beneficial to the data subject as it facilitates informativity, modifiability and controllability while maintaining information security.

Keywords: e-consent, e-health, security, interoperability, privacy by design.

Supervisors	**:**	Prof HS Venter
		Dr G Sibiya
Department	**:**	Department of Computer Science
Degree	**:**	MSc (Computer Science)

Acknowledgements

I would like express my gratitude to:

- My supervisor, Prof HS Venter, for his invaluable guidance. I sincerely appreciate his attention to detail and the investment of his wisdom and knowledge in my research journey.
- My co-supervisor, Dr George Sibiya, for his helpful research insight and input.
- My parents, Dorothy and Simon Zazaza, for their constant love and support.
- My siblings, Yivani and Khungani Zazaza, for unknowingly bringing much-needed humour into my life.
- My partner, Mufaro Mufandaidza for his words of encouragement and always being there to listen.
- The Hore-Nyahwa family for their motivation and delicious food.
- The Council for Scientific and Industrial Research for funding my postgraduate journey; and the care from the Wildcards team and Thomas Fogwill.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

In a world with a population of 7.6 billion, 4 billion people have access to the internet [65]. Africa has seen the fastest growth rates, with the number of internet users increasing by more than 20% each year [85]. In Africa, an individual is more likely to have access to a cell phone service than to piped water, sewage, tarred roads or electricity [85]. The decreasing cost of digital storage and the rise of Internet of Things (IoT) has led to the creation of more data at a faster rate than ever before [130].

The ubiquitous nature of the internet means that over 2.5 quintillion bytes of data are generated per day, equating to 10 million blu-ray disks [122]. Every minute, over 46 000 Uber trips are taken, 3.6 million Google searches are conducted and 103 million spam emails are sent [72]. Given that over 50% of the world's population has access to the internet, there is a growing concern over the privacy of information that resides on personal devices as well as in the cloud.

In 2013 and 2014 Yahoo was a victim of a data breach when 3 billion users' information was compromised [28]. The information involved in the breach included full names, dates of birth, email addresses, passwords, and security questions and answers [28]. Other online services that have experienced data breaches include online dating services, online shopping services (eBay), payment-processing service providers (Heartland Payment Systems), credit bureaux (Equifax), department store retailers (Target Stores), transportation network companies (Uber) and Sony's PlayStation Network, where hackers gained access to information such as purchase histories and credit card numbers [28]. In each of these data breach events, millions of users were put at risk of identity and monetary theft.

Most of the time, consumers are unaware of how much data is collected about them online. An individual's political and ethnic affinity, as well as his or her background is often tracked [132]. Cookies on visited websites aid the process of customised advertising [132]. With the use of technologies such as Bluetooth or Global Positioning System (GPS), retailers are notified when a customer enters the store and they are provided with information such as the customer's income and how often he/she shops [132]. Services such as Google have records of each user's advertisement profile, all the software applications each user has used, the user's whole YouTube history, and Google search queries, as well as all the places they have visited [29]. The risks of consumers' data being collected and used unknowingly by third parties is discussed in more detail in this dissertation.

The remainder of this chapter is structured as follows: Section 1.2 introduces the problem statement and outlines and details the research questions that will guide the research. Section 1.3 provides the objectives of the research and Section 1.4 describes the research methodology. The chapter concludes in Section 1.5 with an overview of the chapters that will be covered in the dissertation.

Giving individuals control over their information and what they choose to share should be aligned with their right to privacy. This concept is inline with the problem this dissertation aims to address, and is discussed further in the following section.

1.2 Problem Statement

In the age of computing, it is becoming more difficult to be in control of the level of privacy of one's information. Information that reside in an individual's medical record is private, and unwanted exposure of that information can lead to reputational harm or emotional distress. There should be a natural understanding that the confidentiality of an individual's medical record is maintained. In South Africa, privacy is a basic human right, so a violation of that right is prohibited. Only healthcare staff who have access to a patient's medical record should be allowed to access it. Consent is not only limited to the control an individual has over his/her information privacy but also allows them to convey and document specific instructions that are related to their medical care.

Given that South Africa and the world are moving towards e-health, there is a need for an approach towards privacy preservation through e-consent. This means that a patient should be given access to an e-consent system for them to express their consent directives. Thus, the problem this dissertation investigates is the efficient and practical application of informed e-consent in e-health in South Africa.

The questions that will guide this dissertation are as follows.

- What is the current state of e-consent in healthcare? This question gives insight into the degree of and utilisation of e-consent systems at healthcare facilities. The accomplishments, challenges and opportunities surrounding e-consent systems are identified, so that a redundant solution by this dissertation is avoided, and instead a new solution is developed that can improve upon aspects that are beneficial to e-consent systems. This question also seeks to identify the perceived value of e-consent to determine whether it is regarded as an essential function.

- What challenges do South African healthcare sector workers experience with regard to e-health? This question identifies whether healthcare-sector workers are equipped with the relevant information and communication technology skills required for them to work with existing e-health systems that are not necessarily e-consent systems. Furthermore, this question seeks to evaluate if the level of training given to the workers is sufficient; if there is sufficient access to Information Technology (IT) resources such as the internet; and whether ongoing information technology support is provided for those systems. This question also identifies the opinions, attitudes and relationships that healthcare workers have of and with e-health systems. If there are challenges that broadly affect e-health systems, it is unlikely that these challenges will not affect an e-consent system. Thus, the challenges that electronic health systems face are identified so that solutions to mitigate the impact of these challenges are applied, where possible.

- How can privacy preservation legislatures such as the PoPIA be applied in e-consent systems? This question seeks to identify the relationship between e-consent and privacy regulations in order to observe whether privacy regulations affect the approaches taken in the development of e-consent solutions. Where limitations exist, appropriate measures should be taken where necessary. In addition, instructions from the relevant privacy legislature should be integrated into the developmental life cycle so that an e-consent solution is developed inline with privacy laws in such a manner that it is of value to healthcare subjects since it is developed with their best interests in mind.

- In what way can interoperable e-consent systems be implemented in South Africa?

This question seeks to identify the standards and implementation guidelines that are available to facilitate the development of interoperable e-consent systems. The significance of interoperability is that it allows different software applications to communicate and exchange information with each other through the use of applicable standards. There are many different e-health systems that exist in South Africa. Consequently, knowing the tools that can aid interoperability means that better communication is possible between different health software applications.

The issues identified in the problem statement are solved by a number of objectives which are discussed in the following section.

1.3 Objectives

The main objective of this dissertation is to design and develop an e-Consent Management System (eCMS) that facilitates customised privacy control for healthcare users who make use of electronic healthcare systems. The specific objectives that are pursued as part of the main objective are as follows:

- Analyse existing work on e-consent, interoperability, information security and privacy preserving legislature and principles.
- Conduct a research survey that will provide information on the current state of e-consent in South Africa.
- Design an e-consent management system model.
- Develop a prototype of the e-consent management system model as proof of concept.

The following section outlines the methods applied to achieve the objectives listed above.

1.4 Methodology

The methods included for this research are the literature review, modelling and prototyping. A more detailed description of these methods follows.

- *Literature review:* A state-of-the-art literature review is conducted on e-health, e-consent, information security and privacy legislature in the South African context. A literature review provides the necessary background and helps identify the similarities, shortcomings and opportunities from the relevant literature. Subsequently, the knowledge acquired from the literature review is used to design the conceptual model.

- *Modelling:* A conceptual model is a visual representation of an idea and it describes the semantics of a system at a high level. The knowledge obtained from the literature review and the statistical results from the survey aid the design of a conceptual model. The model presents an abstraction of the proposed system, whose function is to facilitate customised privacy control for healthcare users using electronic healthcare systems.

- *Prototyping:* A software prototype for the designed conceptual model is developed using the relevant programming languages, application programming interfaces and integrated development environments. Prototyping allows for a software artefact to be developed and tested as specifications of the system are gradually obtained. A prototype puts into practice the guidelines obtained from the literature and the model; subsequently, the feasibility and shortcomings of the artefact are identified when the prototype is used to simulate real-world situations.

The outline of the dissertation follows in the subsequent section.

1.5 Dissertation Outline

This dissertation consists of eight chapters. The current chapter, **Chapter 1**, provides an introduction to the study. A brief overview of the background to the research is covered. Following this, the objectives of the study are discussed, and the problem statement and research questions are outlined. The rest of the dissertation is organised as follows:

Chapters 2 and 3 provide the literature reviews for the e-health, consent and privacy concepts. The chapters provide the necessary background information for the areas of interest discussed in the dissertation.

- **Chapter 2** begins with a description of the South African healthcare system, explaining that it comprises of the private and public healthcare systems. The chapter continues to explain how the need for e-health has arisen due to the workforce strain experienced by the public sector. Furthermore, the chapter discusses the opportunities, challenges and solutions faced by e-health in South Africa. The chapter also provides background on consent and explains the significance of obtaining informed consent from patients, as well as the repercussions for service providers who do not respect the privacy of their patients. The chapter then introduces electronic consent and discusses its advantages over written consent. The rest of the chapter provides an overview of consent directive types, attributes and controls.
- **Chapter 3** covers information security with a specific focus on principles and legislatures that are essential for privacy preservation such as the Protection of Personal Information Act, the Health Professions Act and the General Data Protection Regulation. Information security and e-consent go hand in hand as both concepts strive to ensure data privacy. Later in the chapter, the focus shifts to

access control with a discussion of the types of access control techniques that exist as well as which are better suited for e-consent systems. The chapter also provides a discussion of related work. The chapter compares the model and prototype developed for the research against other literature studies which have conducted similar work. Furthermore, the chapter identifies the ways in which the developed prototype is better than other e-consent implementations.

Chapters 4 to 6 present the contribution of the research which includes the e-consent management system model, design and the software prototype.

- **Chapter 4** proposes a model for the e-consent management system. The model is designed based on the information gathered from the literature reviews (Chapters 2 and 3). The model presents an abstraction of the proposed system, the function of which is to facilitate customised privacy control for healthcare users that makes use of electronic healthcare systems. The chapter also illustrates the architectural design of the e-consent management system based on the conceptual model.

- **Chapter 5** describes the implementation of the software prototype developed based on the e-consent conceptual model. The relevant programming languages, application programming interfaces (APIs) and integrated development environments (IDEs) are described. In addition, the standards and implementation guidelines that were used during the development process are mentioned.

- **Chapter 6** demonstrates the consent directive life cycle, by way of a scenario, by detailing its creation, retrieval, update and removal workflows.

Chapters 7 and 8 evaluate and conclude the research.

- **Chapter 7** provides an evaluation of the designed model, architecture and developed software prototype. Furthermore, the benefits and shortcoming of the research are discussed.

- **Chapter** 8 provides the conclusion of the dissertation and discusses future work.

The appendices provide the acronyms, and the publications derived from the research.

- **Appendix A** provides a list of the important acronyms used or newly defined in the course of this work, as well as their definitions.
- **Appendix B** presents the publications that were derived from the work presented in the dissertation.

Chapter 2

e-Health and e-Consent in South African Healthcare

2.1 Introduction

Information and Communication Technologies (ICTs) have become considerably useful over the years as they have played a role in improving the quality of life of individuals. The ICTs use technologies such as the internet, wireless networks, cellphones and other communication mediums [68] to generate, transmit, store and access data. An advantage of ICTs is that they allow solutions to be reached much sooner than if they were done by humans alone. Furthermore, ICTs allow effective and economical solutions to be realised [58].

Given their resourcefulness, ICTs have been utilised to improve the quality of service in areas such as agriculture [5], education [10], construction [93] and transportation [41]. The focus of this chapter; however, is the application of ICTs in the health context, as well as how ICTs aid the advancement of quality healthcare. Formally, e-health is defined as:

"*the combined utilisation of electronic communication and information technology to generate, transmit, store and retrieve digital data for clinical, educational and administrative purposes*" [102].

e-Health is further explored in the remainder of this chapter which is structured as follows: Section 2.2 describes the general state of e-Health in South Africa. Section 2.3 describes the concept of electronic consent in the healthcare context. The chapter concludes with a summary in Section 2.4.

2.2 South African Healthcare System

This section provides an overview of the South African healthcare system, as well as a discussion of the significance of e-health in South Africa.

The South African healthcare system comprises the private and public healthcare system [116] where there are approximately 4 200 public and 800 private healthcare facilities [55]. The public healthcare system serves a significant proportion of the population, but is consistently underfunded and understaffed [116]. About 21% of doctors work for the public sector [116], leaving it poorly resourced and under pressure to serve 82% of the population [104].

In contrast, the private healthcare system attracts 79% of the country's healthcare professionals as it tends to offer better salaries and better working conditions [76]. Table 2.1 shows the ratio of healthcare practitioners to patients in each of the country's provinces. From Table 2.1, it can be observed that, in each of South Africa's provinces there is an understaffing problem of doctors and nurses as - on average - there is one doctor available for every 4 024 patients and one nurse is expected to treat 807 patients. The private

Province	Patient-to-doctor ratio	Patient-to-nurse ratio
Eastern Cape	4 280 to 1	673 to 1
Free State	5 228 to 1	1 198 to 1
Gauteng	4 024 to 1	1 042 to 1
KwaZulu-Natal	3 195 to 1	665 to 1
Limpopo	4 478 to 1	612 to 1
Mpumalanga	5 124 to 1	825 to 1
North West	5 500 to 1	855 to 1
Northern Cape	2 738 to 1	869 to 1
Western Cape	3 967 to 1	180 to 1
South Africa	**4 024 to 1**	**807 to 1**

Table 2.1: Public sector patient-to-doctor and patient-to-nurse ratios by province, 2015 [116]

healthcare system has the added benefit of accommodating high-income individuals who are usually members of medical aid schemes [76]. In order to bridge the gap between the quality of healthcare for patients who use public and private healthcare services, the South African government plans to adopt the National Health Insurance (NHI).

The NHI aims to provide quality and affordable healthcare for all South Africans based on their health needs, irrespective of their socio-economic status [121]. South Africans will be taxed for the NHI service and their contributions will be used to improve and maintain the quality of service of healthcare in the country.

Until the vision of the NHI is realised, factors that contribute to the low quality of healthcare in South Africa are the challenges that come from staff shortages, poor management and weak healthcare [102]. In parts of the country where there is no access to health facilities, e-health technologies can assist those communities by providing equivalent or similar aid [74, 104]. The following section discusses the benefits that are available when e-health technologies are adopted.

2.2.0.1 e-Health Opportunities

e-Health can be used to bridge the gap between developing and developed healthcare facilities [101, 102]. The use of ICT solutions in healthcare provide the following benefits [74, 102]:

Enhanced quality of healthcare:

- Telemedicine and mobile medical care and health management;
- Blood information management.

Reduced costs:

- Anti-counterfeit of medical equipment and medication;
- Medical equipment and medication traceability.

Elimination of errors:

- Real-time monitoring;
- Error prevention mechanism of pharmaceutical preparations;
- Neonatal anti-theft;
- Alarm systems.

Quicker healthcare:

- Information sharing.

Improved storage and access of health-related information:

- Patient information management;
- Medical emergency management;
- Medication storage management.

The use of e-health systems saves time and lives, while reducing nurses' workload [102]. Integrating ICTs into healthcare also allows for the data collected to be used for analyses, thus allowing for better decision-making, resource allocation, taking preventative measures and reducing operational costs [35]. However, even when ICT solutions are implemented, their value can only be realised if they are effectively and consistently used by the people for whom they were intended.

Two variables affect the effective use of ICTs: the Perceived usefulness (PU) and the Perceived ease of use (PE) [102]. The PU refers to end-users appreciating the need for the ICT and the PE refers to how easily an end-user can use a system [80]. If the PU and the PE are absent, the benefits of ICTs cannot be sufficiently realised because its end-users do not value the technology or simply do not use the system because it is too complex; or there is a lack of user training and knowledge transfer [102].

Challenges to the adoption of e-health systems in South Africa include the absence of ICTs at healthcare facilities, staff lacking ICT-related skills and old and unreliable computer equipment [104]. Additionally, 72% of physicians fear that that e-health systems may lead to frequent downtime, and 64% of them believe that productivity may be hampered. However, there is a willingness by staff members to learn to use e-health systems [104].

The next section provides an overview of e-health solutions that are currently adopted in South Africa.

2.2.0.2 General e-Health Solutions

The ICT methods that are currently available in e-health [102] include, but are not limited to, the following:

- *Electronic Health Record (EHR):* An electronic version of a patient's medical information which is easily shared among authorised healthcare personnel.
- *Health Information System (HIS):* Any system that captures, stores, manages or transmits information related to the health of individuals or the activities of organisations that work within the health sector.
- *Telemedicine:* The remote diagnosis and treatment of patients by means of telecommunications technology. Telemedicine is particularly significant for communities in South Africa where the nearest hospitals and clinics are located far away from them.
- *Patient portals:* A secure online website that gives patients convenient, 24-hour access to personal health information from anywhere with an internet connection.
- *Smart cards:* A device with the dimensions of a credit card that uses a small microchip to store and process data, specifically healthcare data in this context.

The above solutions are not well known or widely used in developing areas of South Africa [102] due to technological and non-technological challenges [123] exacerbated by the absence of a uniform approach to healthcare [102]. The lack of standardisation and integration with ICTs brings barriers to the potential that ICTs can provide [102].

Other factors include the lack of ICT equipment, ICT-related skills and adequate maintenance [102, 110]. However, the South African government is still attempting to develop solutions that can mitigate these challenges.

2.2.0.3 Current South African e-Health Solutions

Some of the ICT implementations currently used by the South African Department of Health are listed below.

- *Pharmacy Dispensing Unit (PDU):* This is a self-service machine where patients obtain their prescription medication [109] in a manner similar to that in which money is withdrawn from an Automatic Teller Machine (ATM). To use the machine, the patients scan their Identity Document (ID) or insert a pharmacy card (received during registration) and enter the required Personal Identification Number (PIN) [115]. The medication is then dispensed robotically, based on the selected prescription, eliminating the need for patients to wait in long queues [92]. The PDU system is run by qualified pharmacists who load the prescriptions onto the system and are available through video conferencing during the transactions [109].

- *Stock Visibility System (SVS):* This is a mobile application that reports medicine availability information at primary healthcare facilities [54]. A facility smartphone camera scans the medicine barcodes and automatically updates stock levels accordingly ensuring that medication is timeously ordered and that stock-outs at primary healthcare facilities are reduced [54]. The system helps with demand planning which is particularly important for millions of South Africans who rely on Antiretroviral (ARV) and Tuberculosis (TB) medications [54]. In addition, the SVS assists government in accurately budgeting for healthcare and prevents supply chain mismanagement [63].

- *MomConnect:* This is a free Short Messaging Service (SMS) service that provides pregnant mothers with regular foetal development updates and reminders for clinic appointments in all 11 official languages [105]. One of the objectives of the service is to help reduce the prevalent maternal and child mortality rate in South Africa [44]. Once the baby is born the service updates the mother for up to a year with information on topics such as breastfeeding, when the baby should begin eating solids, immunisation and family planning [44]. Over 1 770 000 unique mobile phone numbers were registered on the service by 2017 [105].

- *Medication Adherence App:* This is a mobile application that reminds users when to take their scheduled medication and when their next visit to a clinic or hospital is scheduled [91]. Human Immunodeficiency Virus (HIV)-positive pregnant mothers can be reminded to take their medication if they have forgotten in order to prevent mother-to-child transmission [91]. Given that an estimated 7.7 million people in South Africa are infected with HIV (the highest number in the world) [69], the medical adherence application is essential in helping users undertake ARV therapy.

- *Health Patient Registration System (HPRS)* - This is an electronic system for the registration of patients at healthcare facilities across South Africa [125]. Each patient added on the HPRS is assigned a unique patient identification number - also known as the Master Patient Index (MPI) [64]. Using the MPI, all the demographic information linked to the patient can be identified and the MPI can be linked to a patient's EHR [64]. The HPRS is installed in at least 3 000 clinics and has registered at least 44 000 000 patients in the country [77]. The system is considered to be the most reliable source of patient demographic information [125].

- *Mothers2Mothers (m2m):* This is a service that connects new HIV-positive mothers to experienced mentors to help expectant mothers during their pregnancy and after delivery [9]. Through the "Electronic Client Appointment Diary", mentor mothers (who are HIV-positive women) help their mentees adhere to drug regimens by providing supportive supervision [20]. Given that females aged 15 to 24 account for 74% of new HIV infections compared to 26% of their male counterparts in sub-Saharan Africa [20], the m2m programme is essential in educating these women on HIV when they fall pregnant so that they do not infect their babies. It also reminds them to take the necessary drugs to prevent mother-to child-transmission.

- *B-Wise:* This is a youth-focused online service that was launched in 2015 to provide young South Africans with information and expert advice on topics such as sexually transmitted diseases, substance abuse and psychological health [87]. The users can post questions related to their health and receive answers from experts within 48 hours [87] In 2016, B-Wise had over 58 600 users and submitted 526 questions and comments to health experts and [87].

In 2013, there were at least 42 different HISs in operation in the public healthcare sector [125]. While the presence of the abovementioned ICT implementations (and the previously mentioned 42 HISs) do not yet work together in a completely homogeneous way, they afford end-users the benefits that are intended by the e-health practice. These benefits improve the quality of service that is provided to healthcare users. The growing acceptance, use and understanding of e-health will ensure that the level of healthcare improves in South Africa.

The next section provides an overview of electronic consent in healthcare. A description of healthcare e-consent directive components follow, namely the formats, types, attributes and controls.

2.3 e-Consent in Healthcare

Health Information Systems (HISs) have enabled healthcare staff to gain easier access to patient information. However, they have also introduced the risk that patient information may be accessed by unauthorised personnel [25]. For this reason, patients should be informed not only why their data is being collected, stored and processed, but also who is accessing it [19]. Such a requirement needs to be enforced through consent policies that allow the patient to permit or deny the disclosure of particular medical information from particular personnel [17, 25, 49]. Patients can choose who may access their medical information such as their HIV/AIDS status, previous abortions, substance abuse, psychiatric illnesses and genetic predisposition to diseases [34, 38, 94]. The improper disclosure of such sensitive information can influence decisions about a patient's education, access to credit or employment, and may even expose the patient to reputational or personal harm [38, 100].

Informed consent is a constitutionally protected right in South Africa; yet, a knowledge deficit exists in terms of the laws and regulations of the country [24]. In the case of *Minister of Safety and Security v. Xaba*, the court refused a court order request by the police for the extraction of a bullet to be used against the accused as evidence connecting the accused to a motor vehicle hijacking [24]. The decision was made because the court order would violate the accused's right to security and control of one's body [24].

An HIS has the obligation to protect a patient's consent rights [19], and when the effective enforcement of consent directives prevents undue disclosure of information, patients gain greater trust in electronic health record systems [53]. In addition to ensuring the privacy of patient data, obtaining informed consent reduces medical errors such as incorrect medical dosages and consequently reduces the number of medical malpractice claims [127].

South African doctors have cited challenges in the handwritten or verbal informed consent process. These have included language and cultural barriers, the lack of interpreters, and workload and time constraints [24]. A high workload prevents a doctor from spending more time explaining procedures even though doctors acknowledge that, ideally, at least 30 minutes should be spent counselling a patient and allowing enough time for questions and clarifications [24]. While doctors have a basic understanding of informed consent requirements, their practical implementation is lacking [117]. About 24% of doctors spend less than five minutes informing the patient, while 53% of doctors spend between five and ten minutes informing a patient [24]. Furthermore, doctors have found the current consent forms to be inadequate because they do not provide the opportunity to explain the detailed complications of a procedure [24]. Patients agree to a procedure even though they do not understand its full implications [59]. A tailor-made consent approach may improve the patient's understanding [59]. Only 21% of doctors disclosed all the risks to a patient [24], while 78% of patients want to know all material risks [23]. Additionally, doctors found that the forms do not consider cultural values, language and privacy [23].

In healthcare, e-consent is the agreement given by a patient through electronic media for medical processes. The e-consent of a patient is represented through his/her set of consent directives, where a consent directive is defined as an instruction given by a patient to a healthcare provider. Besides permitting or prohibiting the collection, access, use and disclosure of private health information, three other forms of consent directives exist: medical treatment consent, research participation consent, and advanced care consent. It is imperative that a patient's consent be unambiguous, informed and given freely [1, 49, 67] – furthermore, it must be as easy to revoke consent as it is to give it [67].

Consent is considered informed when the patient is provided with sufficient information on the relevant processes, when adequate opportunity is given to the patient to consider alternative options, and when all the patient's questions have been answered [62].

2.3.1 e-Consent Healthcare Directive Components

This section discusses the components that comprise a consent directive; specifically, its formats, types, attributes and controls. The application of the consent directive components ensures that the requirements of a consent directive are easily identifiable and fulfilled.

2.3.1.1 Consent Formats

This section discusses the three formats of consent: implied, verbal and written [46]. Implied consent is the most frequently applied in the day-to-day functioning of a health facility, followed by verbal consent and then written consent [47]. An overview of the three consent formats follows below.

2.3.1.1.1 Implied Consent

Implied consent is given when the patient indicates agreement to a health practitioner's instructions (e.g. extending the arm to provide a routine blood sample for testing; taking or swallowing medication provided; attending an appointment for the purpose of receiving information or advice regarding the management of a current condition) [46]. Implied consent is only used for common and non-invasive procedures [47], such as the ones mentioned above.

2.3.1.1.2 Verbal Consent

Verbal consent is when oral confirmation is given for a low-risk treatment or procedure [46]. Examples of procedures that may only require verbal consent include chest X-rays, the insertion of a catheter, the application of wound dressings and the examination of genitals or the rectum [47]. Verbal consent is recorded in the patient's medical record [47].

2.3.1.1.3 Written Consent

Written consent is where the patient signs a document to confirm that he/she has entered into an agreement for a high-risk treatment or procedure [46]. Written consent is further categorised into paper-based and electronic formats. With the introduction of e-health, physical signatures are no longer compulsory, and electronic signatures or activities such as ticking a box are acceptable [74]. Electronic consent can also be realised through tele-consent, where video media are used to facilitate the consent process. Even with the adoption of e-health, patients still give written consent primarily through the signing of physical documents [34, 62, 127]. However, the continued use of physical documents is not ideal. Paper and printing costs are expensive due to the manual nature of the printing process [127]. Physical documents make patient information difficult to store, search and retrieve [62], and it is difficult to enforce access control for physical documents as they are more easily accessible for healthcare staff on the premises as they work there [34]. Furthermore, forms filled in by hand are often incomplete, inaccurate or illegible. This hinders instructions on the form from being carried out [108]. In contrast, an electronic consent management system is considered a more efficient and reliable approach [33] as it is less expensive, more secure and the directives are captured and stored electronically making them easier to retrieve and apply.

The next section describes the category of reasons for which consent may be required.

2.3.1.2 e-Consent Directive Types

In e-health, four directive types exist, as listed below, where each directive type has its own set of requirements [50].

- The privacy directive involves the collection, access, use or disclosure of patient information such as demographic data and medical history.
- The medical treatment directive is an agreement to undergo or reject specific medical treatments such as surgery, non-routine blood tests and high-risk drug administration.
- The research participation directive involves clinical trials and information gathering. A research participant should be informed of the scope, risk and duration of the study, as well as how his/her information and/or tissue or blood samples may be used.
- Advanced care directives include do-not-resuscitate orders, do-not-intubate orders and other end-of-life directives that may relate to the patient's values and beliefs.

The next section provides an overview of e-consent directive attributes.

2.3.1.3 e-Consent Directive Attributes

An e-consent directive should also specify the subject of care, the grantee, the purpose and the time period covered by the consent. The components of an e-consent directive should satisfy the following questions [50]:

- Who is the subject of the directive?
- For which purpose is the e-consent is?
- Who is requesting the e-consent?

- How long will the directive be valid?
- What are the stipulated terms and conditions?

The next section discusses consent directive controls.

2.3.1.4 e-Consent Directive Controls

Healthcare users have expressed the need for greater control over their consent directives [74]. This can be accomplished by adopting an individualised and transparent approach for each patient. Consent forms should be tailored for each patient [108] so that each component on the form is non-generic, relevant and complete. The patient should be able to express any of the consent controls, such as “no consent”, “opt-in”, “opt-in with exceptions”, “opt-out” or “opt-out with exceptions”. This freedom is similar to social media privacy control settings and, coupled with transparency and usability, autonomy is given to the healthcare user.

2.4 Summary

This chapter provided an overview of the structure of the South African healthcare system, highlighting the underfunding and understaffing strains faced by the public healthcare system. The section that followed discussed the benefits e-health brings to healthcare, such as the enhanced quality of care, reduced costs, elimination of errors, speeding up of healthcare services and better storage and access of health-related information. In the subsequent section listed and discussed e-health solutions that are currently adopted in South Africa.

Thereafter, the section that followed provided an overview of electronic consent in healthcare. A description of healthcare e-consent directive components followed, namely the formats, types, attributes and controls. The next chapter concludes the literature review component of this paper by providing the necessary background on information security.

Chapter 3

Information Security and Privacy in Healthcare

3.1 Introduction

Patients are the rightful owners of data that resides in Health Information Systems (HISs), subsequently they may decline to disclose information that they feel may lead to discrimination or stigma [36, 40]. When patient data is protected, patients gain greater trust in e-health systems and healthcare professionals [42, 66, 124]. Beyond personal healthcare, information obtained from a patient's health record may be used for medical research, marketing or life insurance purposes [107]. Giving individuals control of their health information increases the quality and reliability of health data and it reduces the occurrence of malpractice. When the quality and reliability of health research data is improved, the quality of healthcare is ultimately also enhanced [51].

An e-consent system needs to function beyond its responsibility to manage consent directives. It also needs to be supported by security services and mechanisms that prevent unauthorised access to patient information [25]. Such security services ensure data confidentiality, data integrity, as well as data availability [25, 70]. The aforementioned security services are also known as the CIA (confidentiality, integrity, availability) triad and are the pillars of information security [86]. More fine-grained security services are known as identification and authentication, access control (also known as authorisation), non-repudiation and information privacy. Security services are implemented through security mechanisms, where some examples include password protection, encryption, hashing and audit trails, which are used to monitor fraud and abuse, and to prevent the unauthorised use and disclosure of data [51, 66, 124]. These approaches are essential, as insufficient data protection may subject a patient to embarrassment, social stigma and discrimination [42].

The remainder of this chapter is structured as follows: Section 3.2 provides an overview of information security services and their significance in the e-health context. Auditing in HISs is discussed in Section 3.3 as a means to facilitate accountability and the chapter concludes with a summary in Section 3.5.

3.2 Information Security Services

Information security is the practice of defending information from unauthorised access, use, examination, disclosure, modification, copying, moving, or destruction. [81]. Information security is achieved through the application of specific fundamental security services, namely identification and authentication; access control; confidentiality; integrity; non-repudiation; availability and information privacy [86]. These concepts are discussed in the subsequent sections where each section begins with a definition of the security service followed by the mechanism(s) that can be used to achieve the service.

3.2.1 Identification and Authentication

Identification and authentication refers to the process where a known individual on a system is identified and it is verified that he/she really is who he/she claims to be [86]. Once the individual is successfully identified and authenticated they may be given access to the system.

Common identification and authentication mechanisms include, but are not limited to, the following [86]:

- *Usernames and passwords:* A username is the name given to a user to uniquely identify him/her on a computer system and a password is a string of characters used to verify the identity of a user when they try to access the computer system.
- *Logon tickets:* A ticket is issued to the user when he/she logs onto an application. If the user then tries to access a different application, he/she does not need to login again if the applications are linked to each other.
- *X.509 certificates and public key infrastructure:* These are used to verify that a public key belongs to the same computer or individual specified on the certificate.
- *One-time passwords:* passwords that can only be used once to access a computer system or resource, and then expire and can not be used again.
- *Biometrics:* Fingerprint, facial and retina scanning are some of the ways biometrics are used to uniquely identify and authenticate an individual attempting to access a computer system.
- *Multi-factor:* This is a technique of using two or more of the methods listed above during the identification and authentication process. The multi-factor approach is also referred to as “strong authentication” [113], as using a minimum of two

identification and authentication mechanisms increases the likelihood that the individual accessing the system really is who he/she claims to be. During the strong authentication process, the user may be required to present something they have, e.g. his/her biometrics and something they know, e.g. his/her password [113].

The application of these common identification and authentication mechanisms ensures that only known individuals will be allowed to log on to an HIS [86].

Once a user has been identified and authenticated, he/she is given access to certain functionalities of the system based on privileges or responsibilities they have. This process is facilitated through the application of access control, which is the next information security service to be discussed in the following section.

3.2.2 Access Control

Access control (also known as authorisation) is a security service that limits access to patient information based on restrictions enforced by the HIS [129]. Patient information on an HIS may include confidential information, such as laboratory results, daily drug administration and physician notes [107]. Through the use of access control, HIS users are only allowed to access the patient information necessary for them to do their jobs, as such doctors will have access to clinical data, while their secretaries will not [107]. The main types of access control mechanisms available are as follows:

- *Mandatory access control:* all access to resources is strictly controlled by the operating system based on system administrator-configured settings. It is not possible for users to change the access control of a resource [114]. The operating system will not give a user access to a program or file if he/she does not meet the security clearance to access the resource [26].

- *Discretionary access control:* This allows each user to control access to their own data [114]. Operating systems such as Windows and Linux allow users to specify the access privileges of their files [26], such as read, write and execute.

- *Role-based access control:* This assigns permissions to particular roles in an organisation. Users are then assigned particular roles [114]. As an example, roles for clinical staff and registration staff will differ and. as such, they will not have the same access to resources. Clinical staff may have access to medical records while registration staff will not.

- *Rule-based access control:* Access is permitted to resource objects based on a set of rules defined by a system administrator [114]. These rules are usually based on conditions such as location and time of day. Both rule-based access control and role-based access control can be combined to enforce access policies [97].

- *Attribute-based access control:* Access is permitted through the evaluation of a set of rules, policies and relationships using the attributes of users [97]. As an example, attribute-based access control would require users who are: (1) type employee; (2) belong to the Human Resources (HR) department would have access to the HR/payroll system; and (3) during work hours that are within the appropriate timezone [21].

Once a user is authenticated and authorised on a system, a further requirement would be to ensure that the information that the user interacts with remains confidential and is only useful to the intended recipients. The next section discusses confidentiality as a security service, as well as some of the security mechanisms that can be used to facilitate it.

3.2.3 Confidentiality

Confidentiality is the protection of personal information shared with an individual (such as a physician, therapist or attorney) that cannot be disclosed to third parties without the consent of the patient or client [37]. Confidentiality differs from privacy in that privacy refers to an individual's right to control his/her personal information from the public. whereas confidentiality is an agreement between the individual and a range of authorised persons on how information will be used [103].

Confidentiality is implied for a doctor-patient relationship. Subsequently, if the doctor asks a pharmacist to fill a prescription for a patient's ailment it would not be a breach of confidentiality. However, a doctor informing a patient's boss of the patient's ailment is a breach of confidentiality, as the doctor has not kept the patient's information secret [37].

In the context of e-health, confidentiality can be extended to refer to a person, process, or program that is authorised to access a data item in a particular way [86]. Confidentiality can be accomplished through the implementation of the encryption mechanism. Encryption is an information security mechanism where cleartext is scrambled into a ciphertext using an algorithm and key(s). In order to change the ciphertext back to cleartext, the corresponding key(s) need to be used to unscramble the text.

The types of encryption mechanisms include the following:

- *Symmetric:* Both the encrypter and decrypter have access to the same public key to scramble and unscramble the text [11], this is analogous to all members in a household having the same key to open the lock to the front door. An example of symmetric encryption is Advanced Encryption Standard with Galois/Counter Mode (AES-GCM). The GCM is an AES mode of operation accepted by the National Institute of Standards and Technology [131]. The GCM can detect any modifications to information regardless of accidental or malicious intent [2]. Information integrity is ensured by applying a universal hash function and the encrypted text contains the ciphertext, authentication tag and the initialisation vector [2].

AES-GCM is the focus of this research.

- *Asymmetric:* The encrypter and decrypter have access to different keys where the decrypter uses a paired private key to unscramble the text [11]. Instead of the same key being used to encrypt and decrypt the message (as in symmetric encryption), there is a private key to which only the decrypter is privy. This means that, even if the public key used to encrypt the message is revealed, the message cannot be decrypted without the private key.
- *Homomorphic:* Unlike symmetric and asymmetric encryption, homomorphic encryption that ensures scrambled text can be worked on without compromising its encryption. The structure of the original text is maintained even when it is in its ciphertext form [98].

Encryption is significant in e-health as patient information should remain in a state that is not usable for unintended recipients whether, they are people, processes, or programs. In addition to encryption, it is important to ensure the integrity of information. Integrity is the next information security pillar to be discussed in the following section. It is a security service that ensures that the information is not modified in an unacceptable way.

3.2.4 Integrity

Integrity refers to information that is “precise, accurate, unmodified, modified only in acceptable ways, modified only by authorised people, modified only by authorised processes, consistent, internally consistent, meaningful and usable” [86].

A system that can provide integrity as a security service means that all its information and communication remain in the condition intended by the originator.

Integrity can be achieved through a security mechanism called hashing. A hash is a value generated from a string of text using a mathematical algorithm [111]. Hashing differs from encryption in that the text cannot be unscrambled. Common types of hash algorithms include Message Digest 5 (MD5), Secure Hashing Algorithm (SHA) 1 and Cyclic Redundancy Check (CRC) 32.

Using the MD5 hashing algorithm as an example, the string "Your application has been accepted" can be hashed to the string "2354008942e1a457cfffe67e24964afc".

The significance of hashing is that even when a single character changes within the original string, the hash of the string changes completely as is deliberately intended by the hashing algorithm. If the original string is changed to "Your applicatioN has been accepted" (note that the last letter of the second word is now upper case), then the hash changes to "0630226874cb7da4d0b0c4f9c7398170".

Hashing can be used to ensure integrity as per a brief example described below, where User A sends a message to User B [111]:

1. User A writes a message and generates a hash (referred to as the original hash) for it, using one of the hashing algorithms, and then sends the information to User B.
2. User B receives the communication and creates a hash of the message using the same hashing algorithm as User A.
3. User B then compares the original hash from the communication from User A and the hash he/she has just generated. If the two hashes are identical, the message was not altered.

An HIS that strives to maintain data integrity ensures that all medical and administrative data that resides in it is correct and can be trusted.

While integrity is a security service that ensures that communication has not been altered, a different security service is required to validate that the communication was indeed sent by the originator. The next section discusses how non-repudiation is used as a security service to facilitate authenticity.

3.2.5 Non-Repudiation

Non-repudiation refers to the ability of a system to confirm that a sender cannot convincingly deny having sent something [86]. Non-repudiation provides proof of the origin and integrity of the data, therefore, making the successful denial of who or where a message came from or its authenticity difficult [27].

A common security mechanism that can be used to facilitate non-repudiation is a digital signature. A digital signature is the electronic equivalent of a person's physical signature and it can facilitate non-repudiation as an individual cannot deny the authenticity of his/her signature on a document or having sent the communication [27]. Digital signatures are based on asymmetric cryptography, where the individual who creates the digital signature uses his/her private key to encrypt the information, and only the paired public key can be used to decrypt the information. This process is illustrated in Figure 3.1.

The example below expands the example that was previously introduced in Section 3.2.4, where hashing was illustrated as a security mechanism to achieve integrity. In the example below, User A is still sending User B a message. However, in this example, we illustrate how asymmetric encryption is used in digital signatures to achieve non-repudiation.

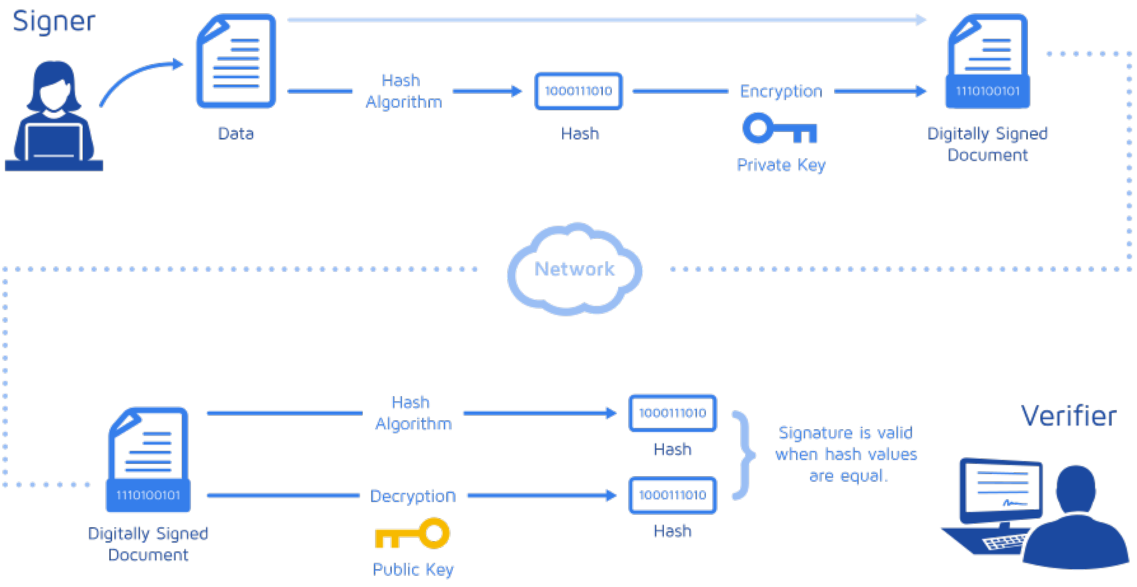


Figure 3.1: The use of a digital signature for non-repudiation [31]

1. User A generates his/her private and public keys using an asymmetric encryption algorithm.

2. User A writes a message and generates a hash for it.

3. User A encrypts the hash using his/her private key and sends the message (which is now signed with the encrypted hash) to User B.

4. User B decrypts User A's hash using User A's public key.

5. User B creates a hash of the message using the same hashing algorithm as User A did.

6. User B then compares the original hash from the communication from User A and the hash he/she has just generated, and if the two hashes are identical, the message was not altered.

In addition to non-repudiation, an HIS needs to ensure that its authorised users can access and utilise its resources when its users should have access to it. Furthermore, a system should guard against security attacks that affect the level of functionality of the system. This security service is referred to as availability and is discussed in the following section.

3.2.6 Availability

Availability refers to the guarantee that authorised persons, processes and programs can get reliable access to information or a service [81].

A service is available if [86]:

- it is present in a usable form;
- it that has capacity to meet the requester's needs;
- it is making progress without errors; and
- it is completed in an acceptable period of time.

Availability is compromised if the system's hardware fails or its operating system environment is compromised.

Security mechanisms that can facilitate availability, include but are not limited to, the following [45]:

- *Redundancy and over-provisioning:* Redundancy refers to the presence of backup resources that can be made available for use in the event of a security attack. Over-provisioning refers to maintaining a system that can handle a greater load compared to how it functions under normal conditions. This can be achieved through the use of powerful servers and faster network connections.

- *Detecting active attacks on availability:* Early detection and quick reaction to availability attacks by system administrators can mitigate the effects of the security attack.
- *Fail safe:* If the HIS is compromised, only the components under attack should be affected.
- *Scalability:* Having an HIS that is scalable means that adding more resources such as servers and bandwidth, will ensure that the system can support the amount of users that utilise it.

An HIS that strives for availability ensures that healthcare staff can access the resources they need at all times, subsequently providing patients with the required quality of service.

The sections thus far have discussed the technical approach towards ensuring information security. The following section discusses information privacy in the context of e-health, as well as which regulations and laws support the protection of patient health information and the application of patient consent.

3.2.7 Information Privacy

Privacy is the freedom from intrusion of an individual's personal matters (such as a medical examination or activities within a home), personal information or any action for which an individual may have the reasonable expectation to deem private [37]. Information privacy usually refers to personal data stored on computer systems. This may include financial records, criminal records, political records, website data and medical records [112].

Privacy differs from confidentiality in that privacy refers to an individual's right to control his/her personal information from the public, whereas confidentiality is an agreement between the individual and a range of authorised persons on how information will be used [103].

Regulations and Acts can be used as mechanisms that enforce information privacy as a service. Some of the South African laws that are in place to protect the rights of individuals include the Health Professions Act and the Protection of Personal Information Act, which are discussed further in the following sections.

3.2.7.1 Health Professions Council of South Africa

Patients are the rightful owners of their data and statutory bodies such as the Health Professions Council of South Africa (HPCSA) (established in terms of the Health Professions Act) aim to protect the public and guide the professions [52]. In healthcare, the implications for practitioners who do not pay proper regard to the privacy of their patients include sanctions from the HPCSA, breach of privacy lawsuits, monetary penalties or even imprisonment [18]. Examples of privacy violations in healthcare include student nurses who capture and share pictures of patients, and health practitioners who may mistakenly disclose patient information without the consent of their patients [84]. Acts such as the Health Professions Act exist to protect patients and ensure that healthcare staff conduct themselves in accordance with the law.

3.2.7.2 Protection of Personal Information Act

The South African Protection of Personal Information Act (PoPIA) is there to protect the processing of information by public and private bodies and to prevent the abuse of personal information by individuals and corporations [18]. The Protection of Personal

Information Act (PoPIA) was partially enacted in 2013. However, it is yet to fully commence due to delays in appointing an Information Regulator and fully enabling its mandate and powers [118]

Obtaining patient information is an integral function of healthcare and it is not illegal provided that patient confidentiality is maintained and patient information is protected [18].

In accordance with PoPIA, examples of illegal patient information processing include the following [18]:

- Taking a photograph with a mobile device of a patient's body without his/her consent.
- Taking a photograph with a mobile device of a patient's hospital record and not ensuring that the image is securely stored.
- Storing patient information on a data-storage device without restricted access.
- Accessing patient information on a public computer and leaving it open.
- Storing patient information for longer than five years without requesting an extension for historical, statistical or research reasons.

The PoPIA is based on the best features of international privacy legislatures and Organisation for Economic Cooperation and Development (OECD) guidelines for the protection of privacy. The PoPIA comprises eight information-processing principles which are summarised below [18, 90]:

- Accountability: The responsible party must ensure that the eight information-processing principles are adhered to.

- Processing limitation: Processing of information must be lawful and personal information may only be processed if it is adequate, relevant and not excessive for the purpose for which it is processed. For example, a health practitioner should photograph only the section of the body that is being treated and not the whole body. In addition, only relevant information required for billing should be provided and not detailed medical information.

- Purpose specification: Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

- Further-processing limitation: Sometimes personal information is received from a third party and must be passed on to the responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected.

- Information quality: The responsible party must take reasonable and practical steps to ensure that the personal information is complete, accurate and not misleading. He/She must update the information where necessary, taking into account the purposes for which it was collected.

- Openness: Personal information may only be processed by a responsible party who notified the Information Protection Regulator in advance. Furthermore, the responsible party must provide certain prescribed information to the data subject (the person or patient involved) by stating what information is collected, and whether or not the supply of the information by that data subject is voluntary or mandatory.

- Security safeguards: The responsible party must secure the integrity of personal information in his/her possession or under his/her control by taking prescribed measures to prevent loss of, damage to, unauthorised destruction of, and unlawful access to or processing of personal data.

- Data subject participation: A data subject has the right to request a responsible party to confirm, free of charge, whether the responsible party holds personal information about the data subject. The latter may also request from a responsible party the record or a description of the personal information held, including information about the identity of all third parties (or categories of all third parties) who have (or have held) access to the information. In addition, a data subject may request a responsible party to: a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading or obtained unlawfully; and b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

3.2.7.3 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a regulation in European law to give members within the European Union and European Economic Area more control over their personal data [83, 96]. Similar to PoPIA, the General Data Protection Regulation (GDPR) requires organisations to collect personal data legally and under strict conditions, for the data to be protected from misuse and exploitation, and for the rights of data owners to be protected [83]. One of the central principles of the GDPR is to increase a data owner's awareness of consent surrounding data processing [74]. Organisations that fail to abide by the regulations will be subjected to penalties [6].

In the health context, the GDPR requires that "data concerning health", "genetic data" and "biometric data" be processed only when at least one of the conditions below are satisfied [96]:

- The data subject must give explicit consent.
- “Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”.
- “Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices”.

In order to ensure that users are using the HIS as they should be, a security service should record all actions taken by the individuals on the HIS. This service is called auditing and is discussed in the following section.

3.3 Auditing in e-Health

Even though an adequate access control mechanism may be put in place, there is still a risk that human factors may affect its ability to protect the consent directives of the patient efficiently [120]. In instances where an HIS user shares his/her password with other parties, the patient information to which the HIS user has access becomes available to unauthorised individuals [120]. Keeping audit logs of the HIS activities; however, may encourage accountability.

Unlike the information security services discussed in the previous sections, auditing does not pro-actively defend information from unauthorised access but rather helps keep track of actions as they happen on a system.

One of the mechanisms that are used to facilitate auditing are audit logs, as they detail who accessed the HIS, when it was accessed and for what reason [36]. Audit logs should be detailed enough [107] and at the same time accessible and understandable by an end-user so that they can identify malicious behaviour [36]. Audit trails assist in disputes [40] concerning the abuse of permissions, illegal access attempts and the improper disclosure of patient data [36].

3.4 Related Literature

This section discusses the related literature on e-consent management in healthcare. To accomplish this task, a literature review was conducted to summarise and provide insight on the information currently available on electronic patient consent management. The eligibility of the information sources were papers that dealt with electronic consent.

3.4.1 Related Work Discussion

This section discusses the methodology followed to obtain literature relevant to the research. The search and comparison criteria are described, followed by a comparison of the studied literature against this research.

3.4.1.1 Search Criteria

The search was conducted by using electronic journal databases such as ACM Digital Library, Elsevier, IEE Digital Library MEDLINE, PubMed, Science Direct and Springer Link between November 2017 and February 2020. Search terms that were applied included patient consent management, e-consent, electronic consent, e-health, privacy and security. Boolean connectors such as AND, OR, NOT. were used on the selected keywords to get more comprehensive search results. The search using these keywords provided 18 studies that met the required criteria. These sources were subsequently evaluated using the comparison criteria.

3.4.1.2 Comparison Criteria

The sources were then compared using the concepts below:

- *Architecture:* This entailed whether the literature considered standards or frameworks to design models or demonstrators as these help to facilitate interoperability in health information systems.
- *Information Security:* This entailed whether the literature had considered information security approaches with respect to consent rules, access control, auditing and encryption.
- *User Involvement:* This entailed that the extent a model or demonstrator described in the literature would ensure the consent the user gives is indeed informed, whether the user would be able to control the settings of his/her existing directives, how the model or demonstrator would handle the grievances of the user and if reports are made available to the user to detail who was accessing his/her information over time.

A complete analysis follows in the next section and is summarised in Table 3.1.

3.4.1.3 Comparison of Studied Literature

Ko and Liou [57] and Heinze *et al.* [49] present studies where patient consent directives in an e-health environment are managed. The platforms are implemented with functionality that allows patients to create, update and revoke their consent directives. The significance of the implementations by Ko and Liou [57] and Heinze *et al.* [49] is that the systems make use of HL7 standards. What is lacking in their implementations, however, is a comprehensive security approach. Ko and Liou [57] highlight that data protection was not considered nor was an auditing process implemented - "personal information may be leaked due to the insecure system ... there is no audit function". Heinze *et al.* [49] highlight that security aspects like logging, authentication and authorisation were not implemented as the system was designed to be "deployed in a closed network".

Can [19] proposes a consent management model where consent policies are created according to privacy concerns and ontology relationships are used to facilitate authorised actions. The proposed consent management model differs from other models in that access control techniques are combined with personalisation aspects based on semantic web technologies. However, the shortcomings of the model are that it does not make use of any standards, frameworks or guidelines and it does not have any ontologies that have been implemented and tested against the model.

Yu *et al.* [128] present an ontology-based framework as well as a prototype system that is based on an open-source EHR system, a generic workflow engine and an ontological rule system. However, the system does not make use of standards, frameworks or guidelines. Instead it is implemented for an OpenMRS system. This means that other HISs cannot (without aid) communicate with an OpenMRS system as their messages will not be of the same formats or types. This diminishes interoperability.

Pruski *et al.* [89] design an e-Consent Rule-Based Language (e-CRL), which included the definition of its syntax and semantics. The e-CRL formalises and facilitates the capture of patients' consent. The e-CRL is similar to the consent directive architecture in that it specifies what attributes the consent should have, i.e. who can access the data, what type of consent (denial or agreement) is necessary, the type and sensitivity of data, the period of validity, purpose, as well as delegation. An example of an e-CRL rule is presented below:

```
WHO (‘radiologist’ & ‘GP’);
WHAT (‘agreement’);
PERM (‘Read,Write,Copy’);
DATA (‘radiological’);
START (05/10/2009);
DURATION (30);
WHY (‘medical control’)
```

The rule above states that individuals who are identified as radiologists or general practitioners are granted permission to read, write or copy the patient’s data, which is of radiological concern. Furthermore, the consent is valid from 5 January 2009 for a period of 30 days and the data may be used for medical control purposes. The shortcomings of the e-CRL is that it has not been implemented for a specific standard, and it has weak security considerations with respect to sensitive health information.

Other researchers propose ways to enforce consent policies for healthcare systems based on workflows [25, 100, 126, 128]. Coiera and Clarke [25] and Rusello *et al.* [100] describe frameworks for obtaining and determining e-consent within e-health, Rusello *et al.* [100] specifically managed patient consent policies through the observation of workflow rules in an e-health environment. The system by Yu *et al.* [126] does not allow for patients to revoke their consent and consent forms are not automatically generated. Workflow-based access control systems are significant. However, none of the aforementioned systems apply to any health information exchange standards or frameworks.

Ruan and Yeo [99] developed UML models for a system which that protects patient beneficiary information using e-consent rules. The UML models depict how access control issues regarding patient information are addressed before the software implementation of the system can commence. While the paper details access control policies via a model, it still needs to "extend and enrich the security requirements specifications" in order to have a more complete security approach.

O'Connor *et al.* [74] propose steps that should be taken when designing and developing a system for data collection and sharing in the e-health context. The paper further highlights the importance of applying privacy by design in light of GDPR. However, it does not offer a complete solution for e-consent management in e-health systems, while considering in-depth security solutions or a solution that facilitates interoperability. However, the paper does not delineate how the consent directives would be structured, how informed consent would be received from the beneficiary and what the auditing process of the system would be or if the e-consent tool would be an embedded aspect of an HIS, which would offer real-time intercession.

Boutin *et al.* [15] developed an electronic informed consent tool to facilitate biomedical research using information from a biobank to attract over one million participants. Biobanks store and process human biological specimens where the specimens may be linked to a beneficiary's EHR. Biobanks are a valuable resource for studies related to rare diseases, disease treatment and innovations that involve personalised medication. Given the nature of information stored in biobanks, informed consent is obtained from participants for the use of specimens, as well as to be contacted again for future studies. Boutin *et al.* [15] acknowledge that a secure and efficient informed consent tool is required to attract many participants. However, since the tool makes use of users that already exist on a different infrastructure, the same username and passwords were leveraged, which means that, if the other system is breached, the e-consent system also becomes vulnerable because there are no additional layers of authentication. Furthermore, the tool developed by Boutin *et al.* [15] is an isolated project that does not promote interoperability between various HISs and there is no standard specified for how the consents were developed. There is also no emphasis on information security or how beneficiaries can report grievances they may have.

Heinze and Bergh [48] present a model for consent-based privilege management, which can serve as a framework for health information exchanges. The paper does not detail the security measures or law and guidelines that motivate its development. The paper does not discuss how informed consent is obtained from the beneficiary and the control they have over their directives afterwards.

O'Keefe *et al.* [79] developed a model and demonstrator for controlling access to EHR information shared between healthcare providers through the use of patient consent. The e-consent model was developed so that various independent HISs can communicate with each other without difficulty. As part of the design, the paper details secure transfer protocols for transferring beneficiary EHR information. The paper highlights that an e-consent system should be technology independent and capable of being used with existing systems. In addition, it should be lightweight and not impede existing HIS workflows. The paper does not highlight how the e-consent tool would ensure that the beneficiary is informed when giving his/her consent or how the system would account for health providers who abuse the directives of their patients. Eskeland and Oleshchuk [34], Madathil *et al.* [62] and Ge *et al.* [39] also implemented consent managements systems. However, none of these studies make use of HL7 or other standards that facilitate interoperability. A summary of the analysis is presented in Table 3.1.

Table 3.1 lists all the related sources and compares each source's architecture, information security and user involvement approach. The check mark (✓) indicates that a feature is implemented. The final row in the table shows which features were implemented by this research - it is evident that this research addresses all the features. Therefore, it is more comprehensive than the listed related sources.

Table 3.1: Comparison of literature approaches

	Architecture		**Information Security**				**User Involvement**			
	Inter-operable	PbD	Consent Rules	RBAC	Encryption	Auditing	Reports	Disputes	Control	Informed
[57]	✓		✓	✓					✓	
[19]			✓	✓					✓	
[25]			✓	✓	✓	✓				
[100]			✓	✓		✓				
[13]			✓							
[49]	✓		✓	✓					✓	
[127]			✓	✓						
[62]						✓				
[39]					✓					
[128]			✓	✓		✓				✓
[34]					✓					
[126]			✓							
[89]			✓	✓						
[99]			✓	✓						

Continues on the next page.

Table 3.1: Comparison of Literature Approaches (cont.)

	Architecture		**Information Security**				**User Involvement**			
	Inter-operable	PbD	Consent Rules	RBAC	Encryption	Auditing	Reports	Disputes	Control	Informed
[74]		✓			✓					
[15]				✓						
[48]	✓			✓					✓	
[79]	✓		✓	✓	✓				✓	
This research	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

3.5 Summary

This chapter provided a brief overview of information security in healthcare. A description of several information security services followed. These were identification and authentication, access control, confidentiality, integrity, non-repudiation, availability, information privacy and auditing.

The chapter also discussed the role of the South African law in e-health and the implications for health practitioners who do not act in accordance with the law. This chapter highlighted that, in order to facilitate informed consent, it is important that policies at healthcare facilities encourage the culture of informing patients about which data the facility wishes to collect, how that data may be used, the purpose of the collection of the data and informing the patient that he/she is an active participant in the process and that he/she can withdraw and ask for changes should he/she wish to do so. An e-consent system can thus be used to facilitate the informed consent process.

Furthermore, the chapter provided an overview of the related literature of the research. Based on the specified search and comparison criteria, papers related to this research were selected. The relevant selected research was then compared with all the comparison criteria in order to measure the total criteria met.

The next chapter commences the first contribution chapter of this research.

Chapter 4

A Conceptual Model for e-Consent Management

4.1 Introduction

This chapter proposes a model for an e-consent management system for HISs. The preceding chapters highlighted the importance of informing patients why and by whom their personal information was being collected and used. Specifically, Chapter 2 defined e-consent in the healthcare context and Chapter 3 discussed the legislation that protects patients from having their information used without their consent.

This chapter presents a model for an e-consent management system with the main function of facilitating customisable privacy control for patients using electronic healthcare systems. The rest of the chapter is structured as follows: Section 4.2 describes the requirements for an e-consent management system. Section 4.2.3 discusses the conceptual model of the e-consent management system. The chapter concludes with a summary in Section 4.4.

4.2 e-Consent Management System Requirements

This section motivates and describes the requirements that the e-consent management system should satisfy.

4.2.1 Motivation

Chapter 2 provided background on e-consent in healthcare with the purpose of defining informed consent and explaining the components that make up the structure of consent directives.

The chapter motivated that e-consent is a mechanism required by patients as the continued use of physical documents is not ideal due to the high nature of paper and printing costs [127], physical documents make patient information difficult to store, search and retrieve [62], and it is difficult to enforce access control in the case of physical documents [34]. Furthermore, forms filled in by hand are often incomplete, inaccurate or illegible. This hinders instructions on the form from being carried out accurately [108]. In contrast, an e-consent management system is considered a more efficient and reliable approach [33] as it is less expensive, more secure and the directives are captured and stored electronically, making them easier to retrieve and apply.

The background derived from Chapter 2 can thus be represented as a taxonomy that illustrates consent in healthcare in Figure 4.1 in a more compact and organised fashion.

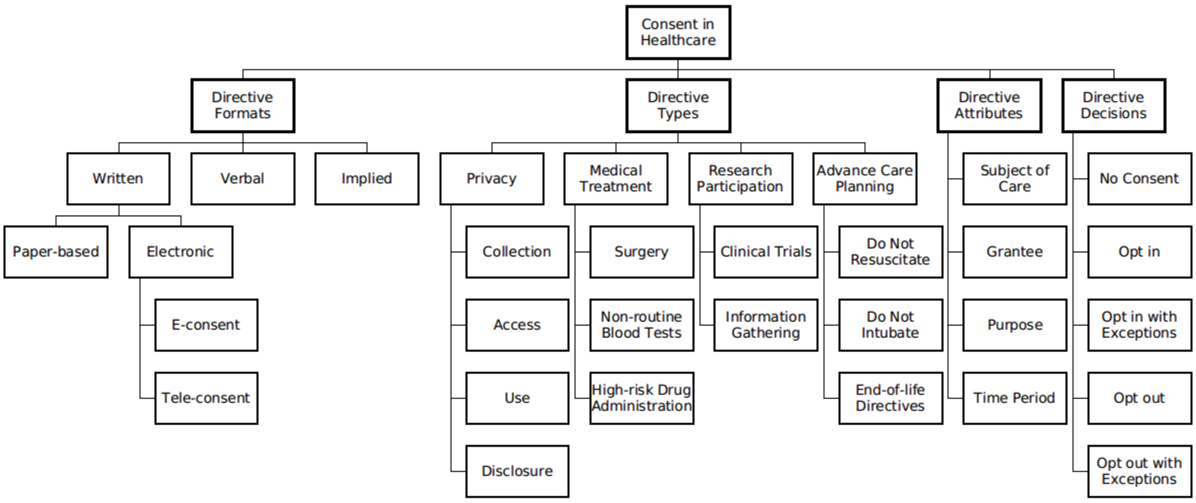


Figure 4.1: Healthcare consent taxonomy

The second level of the taxonomy is made up of the formats, types, attributes and decisions for a consent directive. The directive formats include written, verbal or implied. This dissertation focuses on the application of electronic written consent. The directive types include privacy, medical treatment, research participation and advanced care planning. This dissertation focuses on the privacy directive type with respect to the collection, access, use and disclosure of patient information. The directive attributes include the subject of care, grantee, purpose and time period. The directive decisions include no consent, opt in, opt in with exceptions, opt out and opt out with exceptions.

Chapter 3 provided detailed background on information security in healthcare and highlighted how patient rights are accommodated in South African legislation. Additionally, the chapter explained how security services such as: identification and authentication, access control, confidentiality, integrity, non-repudiation, availability and auditing can be used to protect the patient.

There are four drivers [78] for the development of an e-consent management system:

- *Social:* It has become easier to access health information owing to its electronic nature. Healthcare staff can communicate more easily with each other and they can access information such as medication lists (prescription history details) and problem lists (ailments that affect the health of the beneficiary) quickly. However, the privacy of personal health information needs to be maintained as beneficiaries consider their health information to be among the most private type of information.
- *Economic:* There is an opportunity to mitigate legal actions that emanate from claims of unauthorised sharing of the beneficiary health information. Therefore, it is essential to maintain a record of beneficiaries who have given permission to service providers for the utilisation of their health information.
- *Technical:* Owing to the ease of convenience of copying and sharing information that resides on electronic devices, there is a need to enforce effective access control so that the privacy of beneficiaries is maintained.
- *Legal:* The increase in changes and enforcement of privacy regulations and laws enforces the compliance of data handlers to abide by the directives specified in the laws. Failure to abide by these guidelines may lead to financial penalties or imprisonment.

ISO 27001 is an international information security management standard for the protection of information [30]. ISO 27001:2013 has 14 security controls, which include, but are not limited to information security policies, access control, cryptography and information security incident management [61].

The GDPR offers only the high-level implementation of security management, whereas ISO 27001 clearly lays out the steps to implement a secure system [61]. Organisations that are ISO 27001 certified are halfway to being GDPR compliant [61], and organisations that are PoPIA compliant are 80-90% GDPR compliant [119].

Unlike the GDPR, ISO 27001 does not directly discuss consent, data portability, the right to be forgotten, the right the to restriction of processing, he right to object and the international transfer of personal data [119]. However, ISO 27001 offers technical implementation details. While it does not cover all the aspects of the GDPR to be compliant, it is a valuable step to follow to ensure that the best security measures are implemented [61].

Challenges that are faced when developing an e-consent management system include the following [78]:

- *Challenges with beneficiaries making use of an e-consent channel.* The system will need to be simple enough for beneficiaries to understand what is expected of them, and comprehensive enough for the various aspects of the directive to be captured. Additionally, making beneficiaries aware of the risks involved may make them unnecessarily anxious.
- *Challenges with service providers promoting the use of an e-consent channel.* The system needs to be implemented in such a way that the existing roles and processes across different types of healthcare facilities are accommodated without introducing a large cultural shift. Additionally, the system should be simple enough that healthcare staff can explain it to beneficiaries with ease.
- *Challenges with the technical implementation of the e-consent channel.* The system will need to be flexible enough to accommodate future needs of healthcare facilities. The consent information needs to be securely stored and transmitted, and access to the information should be controlled, considering that even glancing the directive, and not the actual EHR, may still reveal the health status of the data subject. In order to facilitate interoperability, standards need to be followed so that different

HISs that communicate with each other can easily transfer information between one another. The system should also be scalable and perform efficiently to support use by many users.

Following this motivation, the next section discusses the functions an e-consent management system should perform.

4.2.2 List of Requirements

This section presents the requirements that an e-consent management system should satisfy. The PoPIA is based on the eight privacy guidelines of the OECD. The OECD's privacy guidelines provide practical ways for privacy to be facilitated [75]. Given that the PoPIA is based on the best features of international privacy legislation and the OECD's guidelines for the protection of privacy [18], the requirements listed below have been aligned with both the PoPIA and OECD's guidelines in mind. These requirements exist in four broad categories informativity, modifiability, controllability and information security.

Informativity

1. Provide a patient with relevant and qualitative information so that he/she can give his/her informed consent.

2. Provide a patient with the option to receive communication in his/her home language or preferred language.

3. Provide a patient with an avenue to easily ask questions that relate to his/her consent directive.

4. Provide a patient with a report that details requests that were made using his/her consent directives.

5. Notify the patient about any changes requested by the service provider for his/her consent directives.

   Modifiability

6. Allow the patient to easily modify his/her consent directives.

   Controllability

7. Allow the patient to easily give or revoke his/her consent to a service provider. Specifically, a patient can decide to provide no consent, opt in, opt in with exceptions, opt out or opt out with exceptions for a consent directive.

   Security

8. Log all requests made using the patient's consent directives for auditing purposes and to facilitate accountability.

9. Enforce the patient's consent directives at all times.

The next section illustrates the conceptual model of the e-consent management system that will be used to satisfy the above requirements.

4.2.3 e-Consent Management System Conceptual Model

The e-consent management system aims to combine the e-consent functionality of an HIS with functionality that ensures security and interoperability. The following sections describe how the conceptual model for e-consent management is developed and how components of the model link to the requirements listed in Section 4.2.2.

4.2.3.1 Security, Privacy and Consent Dimensions Model

Chapter 3 provided the background for information security services. This includes identification and authentication, access control, confidentiality, integrity, non-repudiation, availability and auditing.

These security services can now be used to enforce the privacy principles mentioned in the PoPIA (see Figure 4.2): accountability, processing limitation, purpose specification, further processing limitation, information quality, security safeguards, openness and data subject participation. Once the security and privacy dimensions have been established, the consent dimension (which offers the informed consent management system functionality) is facilitated by offering informativity, controllability and modifiability.

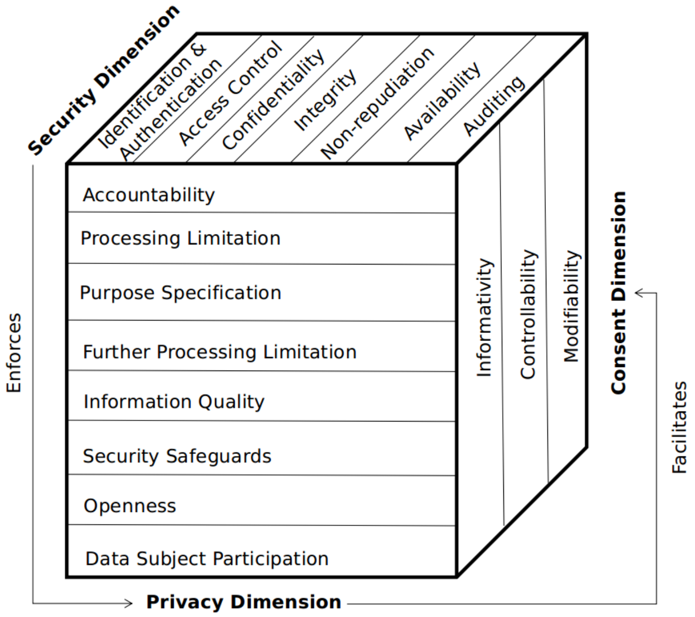


Figure 4.2: The relationship between the security, privacy and consent dimensions

This conceptual model satisfies all the requirements mentioned in Section 4.2.2 at a high level, whereas Figure 4.3 illustrates a taxonomy that satisfies all the requirements in Section 4.2.2 at a more granular level than Figure 4.2. Figure 4.3 shows the security and privacy dimensions as illustrated in Figure 4.2. Additionally, more detailed attributes are represented for the informativity, controllability and modifiability requirements. The taxonomy illustrates that an e-consent management system should securely store informed consent directives that can easily be accessed and reviewed by healthcare users and service providers.

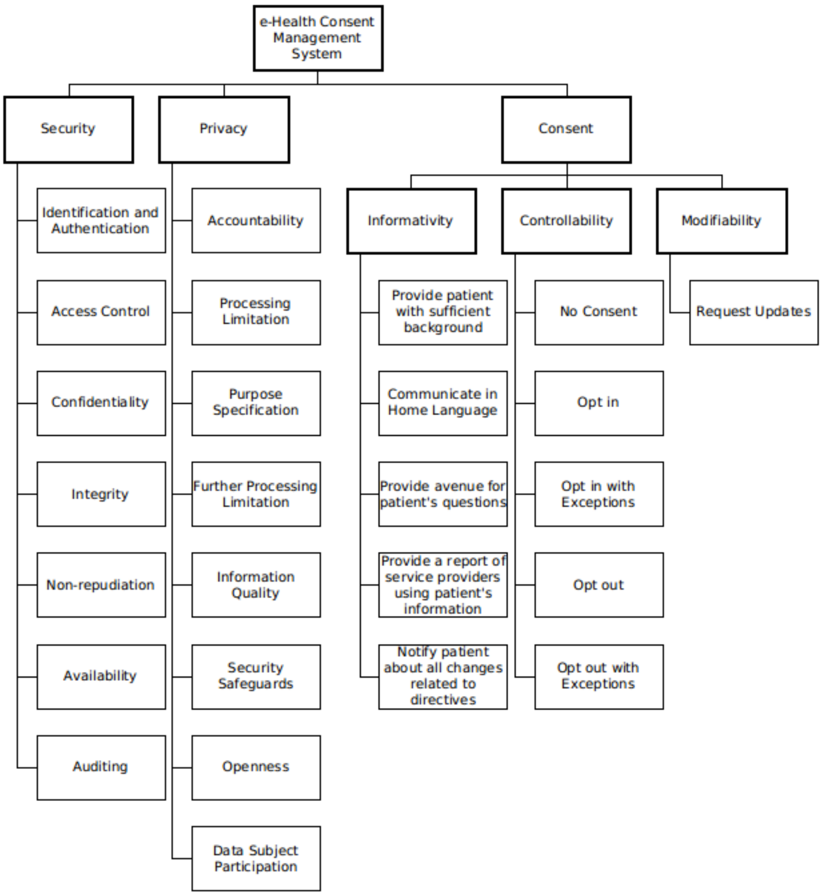

e-Health Consent Management System
Security
Privacy
Consent
Identification and Authentication
Access Control
Confidentiality
Integrity
Non-repudiation
Availability
Auditing
Accountability
Processing Limitation
Purpose Specification
Further Processing Limitation
Information Quality
Security Safeguards
Openness
Data Subject Participation
Informativity
Controllability
Modifiability
Provide patient with sufficient background
Communicate in Home Language
Provide avenue for patient's questions
Provide a report of service providers using patient's information
Notify patient about all changes related to directives
No Consent
Opt in
Opt in with Exceptions
Opt out
Opt out with Exceptions
Request Updates

Figure 4.3: Taxonomy of an e-consent management system

We find requirements the first five requirements from Section 4.2.2, under the informativity category. In order to ensure that a patient is sufficiently informed about the processes he/she needs to participate in, a patient should be provided with sufficient background in his/her home language or preferred language. South Africa has 11 official languages. Only 8.4% of the population speaks English in their homes, while 17.6% of the population speaks English outside the household [4]. Subsequently, automatically delivering formal communication in English is not ideal as the patients are unlikely to fully understand the correspondence. The third requirement specifies that an avenue should be provided for patients to ask questions. This ensures that patients can easily contact professionals to seek clarity surrounding their consent directives.

The last two requirements seek to establish transparency from service providers so that a patient is presented with a report that lists all service providers that are currently utilising his/her personal information. Additionally, the patient should be notified about all amendments related to his/her consent directives.

This next section presents the architectural design of the proposed e-consent management system.

4.3 Architectural Design for an e-Consent Management System

Architectural designing is a significant phase in the software development lifecycle, as it helps software developers understand the business requirements before writing the code for the system. An architectural model is used to conceptually show how the components of the system function and interact with each other so that all stakeholders (the end users, clients, architects, analysts, programmers, project managers, and funders) understand how the system will meet the objectives [99].

The architectural model for this research is developed using Unified Modeling Language (UML). UML is a visual modeling language that is widely industry-accepted to visualise, construct and document software artefacts [12, 99].

The following UML diagrams are used in this research to illustrate the architectural design for an e-consent management system:

- Class diagram [99]: A class diagram portrays the properties of a class (i.e. an object) through attributes, and behaviours through operations. Additionally, class diagrams show the relationships (such as inheritance, association and aggregation) between classes.

- Activity diagram [99]: An activity diagram illustrates the flow of activities in the system.

4.3.1 System Overview

This section illustrates how HISs interact with the e-consent management system. Figure 4.4 shows the high-level interaction that e-health systems will have with the e-consent management system. Health Level-7 (HL7) International is an accredited body that sets up standards for the transfer of clinical and administrative data between healthcare software applications [50]. Given that the mission of HL7 is to develop standards that enable the interoperability of global health data, it plays a significant role in as far as the exchange of communication is concerned. The HL7 standard defines the structure for a consent directive (instruction given to a healthcare service provider by a patient) so that HISs can expect the input to have a specific structure. Figure 4.4 also illustrates that the HL7 standard is used to facilitate communication between e-health systems and the e-consent management system in order for requests against the beneficiary's consent directive to be rejected or approved. The beneficiary registry and electronic health records reside in their respective HISs and the consent management system communicates with the systems using HL7.

In the subsequent section, the various components of the e-consent management system are discussed and illustrated.

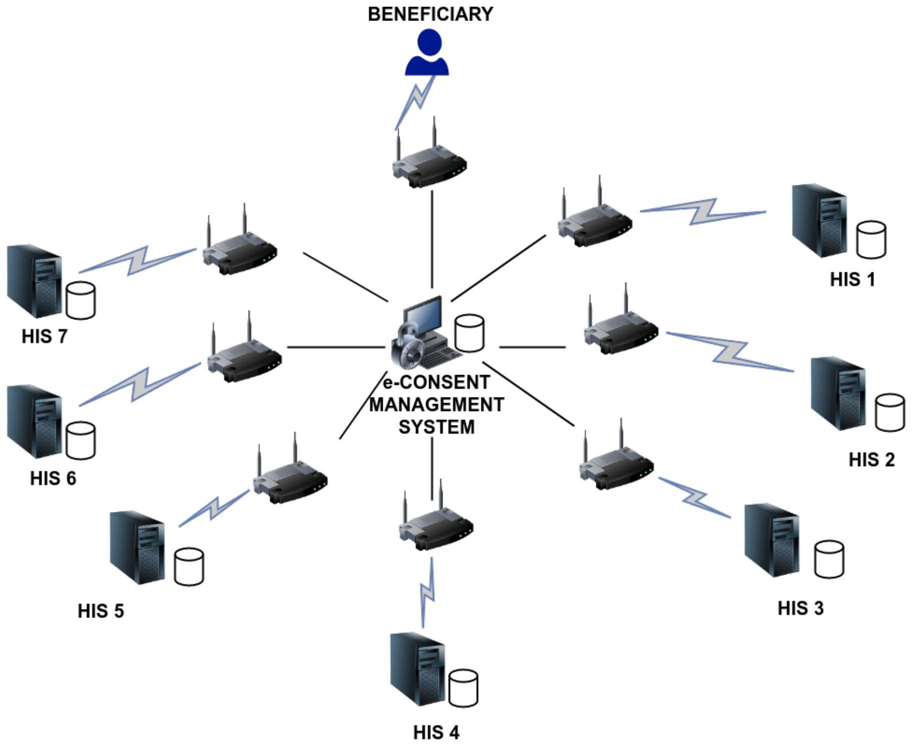


Figure 4.4: The interaction of the e-consent management system with various HISs

4.3.2 Components of the e-Consent Management System

Figure 4.5 illustrates the high-level architecture for an e-consent management system that gives an overview of the components of the e-consent management system and how they interact with one other. The Consent Directive Manager is responsible for authenticating the requester (service provider), notifying the beneficiary (healthcare user) about pending requests and approving or rejecting requests. The figure also shows the Auditor class, which logs the activities of the e-consent management system. The final component is the HL7Formator, which is responsible for standardising the beneficiary consent directives using the HL7 standard.

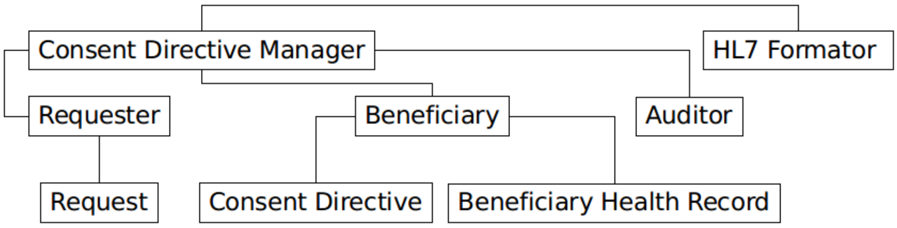


Figure 4.5: High-level architecture for an e-consent management system

In the next section, the e-consent management process is discussed and the interactions among components are described.

4.3.3 e-Consent Management Process

The functions of the e-consent management process include providing the healthcare user with sufficient information to make informed decisions regarding his/her personal health information, generating the necessary consent directives, evaluating all requests made against healthcare user consent directives, and managing consent directives issued by the healthcare user.

To give a logical and consistent explanation of the process described above, we introduce a fictitious scenario that is applied in various contexts to illustrate and discuss the e-consent management process:

> *Jane Smith is a 43-year-old female, who has chronic kidney disease which is the progressive loss of kidney functioning. Until she qualifies for a kidney transplant, she visits the Centre for Renal Care for four hours of haemodialysis (the process of removing toxins and excess waste and fluids from the blood) three times a week. Jane currently has an active consent directive with her doctor (Dr Jacob Fischer) so that he may access her electronic health record and medical history. During a recent examination, Dr Fischer noticed tu-*

mours in Jane's pancreas. In order to determine if the tumors are cancerous or not, Dr Fischer will require input from Dr Maria Roberts, a pancreatic cancer specialist.

This section presents the process of the e-consent management system and discusses the interactions between the requester and consent directive manager. It also considers the interactions between the beneficiary and the consent directive manager. To conclude, the behaviour of the system is illustrated when the requester wishes to access beneficiary information.

4.3.3.1 Interactions Between the Requester and the Consent Directive Manager

Figure 4.6 illustrates the behaviour of the system when the requester interacts with the consent directive manager to create, update, retrieve or remove a healthcare user's consent directive. Figure 4.7 details the relevant attributes and operations involved for the requester and consent directive manager in this context and how they are accommodated in the architecture.

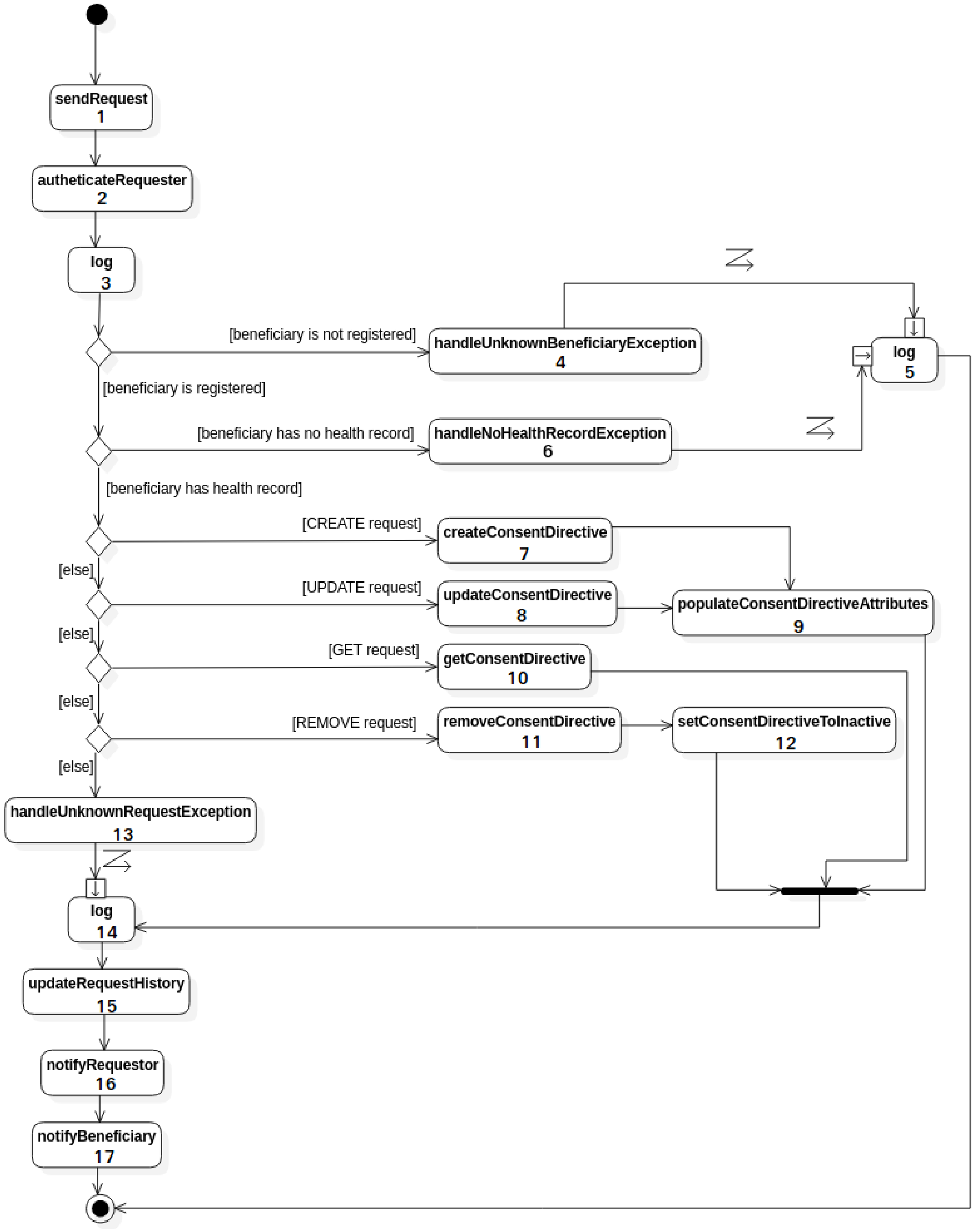


Figure 4.6: Interactions between the Requester and the Consent Directive Manager

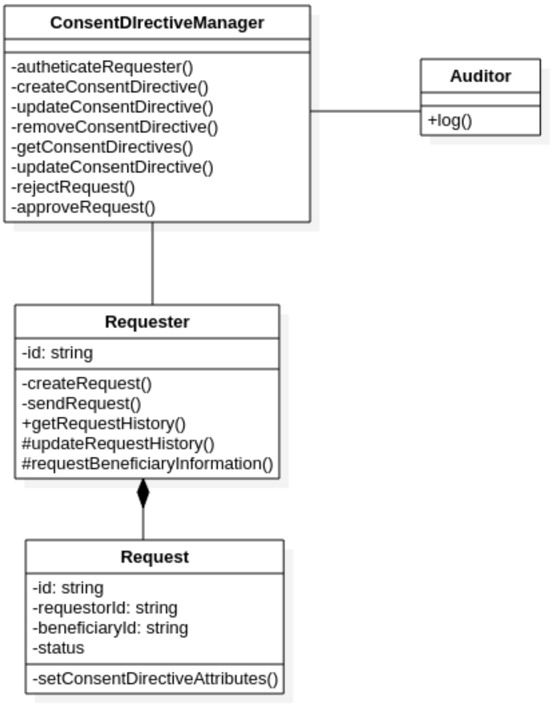


Figure 4.7: Architecture section for the Requester and the Consent Directive Manager

A requester may interact with the consent directive manager to create, remove, retrieve and update a beneficiary's consent directive. Each of these interactions is described in the sections that follow, where Section 4.3.3.1.1 to Section 4.3.3.1.3 give a broad overview of the interactions and Section 4.3.3.1.4 gives specific details related to the scenario introduced in the previous section.

4.3.3.1.1 Consent Directive Creation Workflow

Given that Dr Fischer is currently the sole grantee of the directive, he requires a new consent directive to be created so that Jane can give permission to Dr Roberts, who works at the oncology (cancer) department, to access Jane's electronic health record as he suspects she may have pancreatic cancer and he wishes to refer her to Dr Roberts who is a pancreatic cancer specialist.

Consider a scenario where Dr Fischer makes a request for the creation of a consent directive for his patient, Jane **(1)**[1]. The consent directive manager will begin by identifying and authenticating Dr Fischer to ensure that he is a valid healthcare practitioner **(2)**. The outcome of the authentication process is then logged **(3)**.

The consent directive manager then checks if Jane is registered on the HIS **(4)** and whether she has a health record **(6)**. When both these conditions are met, the workflow for the consent directive creation process begins **(7)**. The consent directive is populated with its appropriate attributes, i.e. the grantee (Dr Roberts), the purpose (access to electronic health record of a patient for a specialised opinion), and the time period (one month) **(9)**. The request is saved, and this action is logged **(14)**. Following the successful creation of the consent directive, the consent directive manager updates the request history **(15)** and Dr Fischer is notified that the request was successful **(16)**. Next, Jane is notified that a decision is required for a new consent directive request **(17)**.

4.3.3.1.2 Consent Directive Removal Workflow

In a scenario where a requester makes a request to remove a consent directive **(1)**, the consent directive manager will begin by identifying and authenticating the requester **(2)**. The outcome of the authentication process is then logged **(3)**. The consent directive manager then checks if the beneficiary is registered on the HIS **(4)** and whether he/she has a health record **(6)**. When both these conditions are met, the workflow for consent directive removal begins **(11)** and the consent directive is set as inactive **(12)**. This action is then logged **(14)**. Following the successful removal of the consent directive, the consent directive manager updates the request history **(15)** and the requester is notified that the request was successful **(16)**. Next, the beneficiary is notified of the action **(17)**.

[1] The numbers in parentheses correspond to the blocks in the process diagram

4.3.3.1.3 Consent Directive Retrieval Workflow

In a scenario where a requester makes a request to retrieve a consent directive **(1)**, the consent directive manager will begin by identifying and authenticating the requester **(2)**. The outcome of the authentication process is then logged **(3)**. The consent directive manager then checks if the beneficiary is registered on the HIS **(4)** and whether he/she has a health record **(6)**. When both these conditions are met, the workflow for consent directive retrieval begins **(10)** and the consent directive is fetched **(12)**. This action is then logged **(14)**. Following the successful retrieval of the consent directive, the consent directive manager updates the request history **(15)** and the requester is notified that the request was successful **(16)**. Next, the beneficiary is notified of the action **(17)**.

4.3.3.1.4 Consent Directive Update Workflow

In a scenario where a requester makes a request to update a consent directive **(1)**, the consent directive manager will begin by identifying and authenticating the requester **(2)**. The outcome of the authentication process is then logged **(3)**. The consent directive manager then checks if the beneficiary is registered on the HIS **(4)** and whether he/she has a health record **(6)**. When both these conditions are met, the workflow for consent directive updating begins **(8)** and the consent directive is updated with the incoming changes **(9)**. The request is saved, and this action is logged **(14)**. Following the successful update of the consent directive, the consent directive manager updates the request history **(15)** and the requester is notified that the request was successful **(16)**. Next, the beneficiary is notified of the action **(17)**.

The following section illustrates and describes the interactions between the beneficiary and the consent directive manager once the beneficiary responds to a request.

4.3.3.2 Interactions Between the Beneficiary and Consent Directive Manager

Figure 4.8 illustrates the behaviour of the system when the beneficiary interacts with the consent directive manager to give a decision to opt in, opt in with exceptions, opt out or opt out with exceptions regarding his/her consent directives. Figure 4.9 details the relevant attributes and operations involved for the beneficiary and consent directive manager in this context and how they are accommodated in the architecture. In this section, we continue with the scenario in the previous section which introduced Dr Fischer, Jane and Dr Roberts.

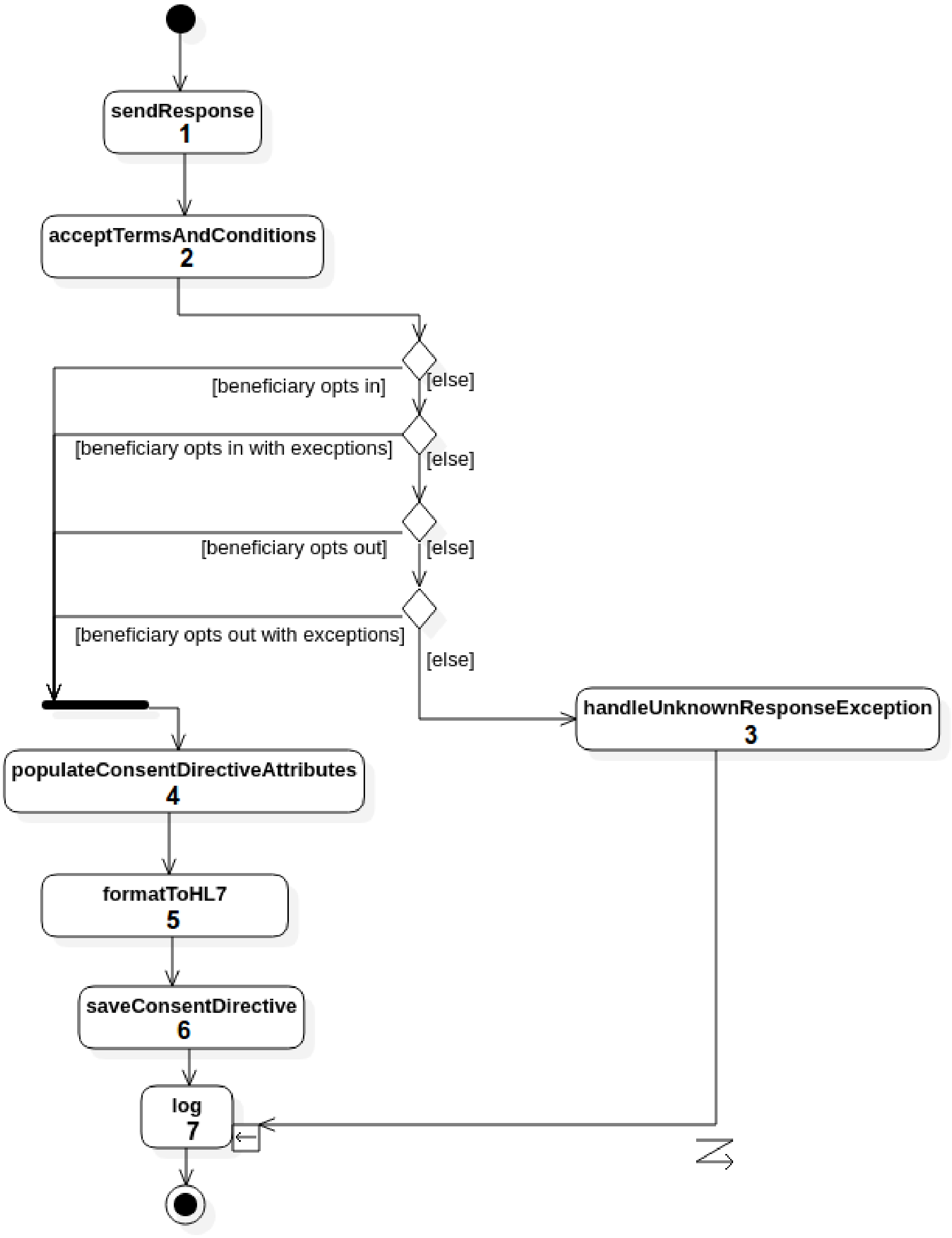


Figure 4.8: Interactions between the Beneficiary and the Consent Directive Manager

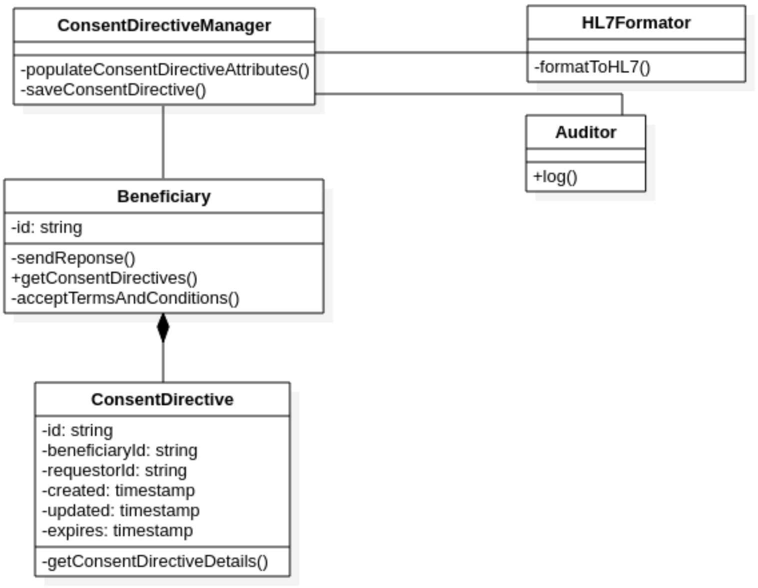


Figure 4.9: Architecture section for the Beneficiary and the Consent Directive Manager

Consider a scenario where Jane decides to give her informed consent to Dr Roberts so that she may have access to her electronic health record **(1)**. The consent directive manager begins by presenting Jane with terms and conditions of the consent directive which will detail the purpose, time period and grantees **(2)**. Once Jane accepts the terms and conditions, she makes a further decision to opt in with the conditions specified by Dr Fischer. The consent directive is then populated with Jane's decision to opt in **(4)** and the consent directive is formatted according to the HL7 standard **(5)** and saved in the database **(6)**. Next, the action is logged **(7)**.

In the next section, we describe the process when Dr Roberts requests information from Jane's electronic health record.

4.3.3.3 Requesting Beneficiary Information

Figure 4.10 illustrates the behaviour of the system when the requester interacts with the consent directive manager to request beneficiary information. It also shows how the consent directive manager either approves or rejects the request. Figure 4.11 illustrates all the components of the e-consent management system.

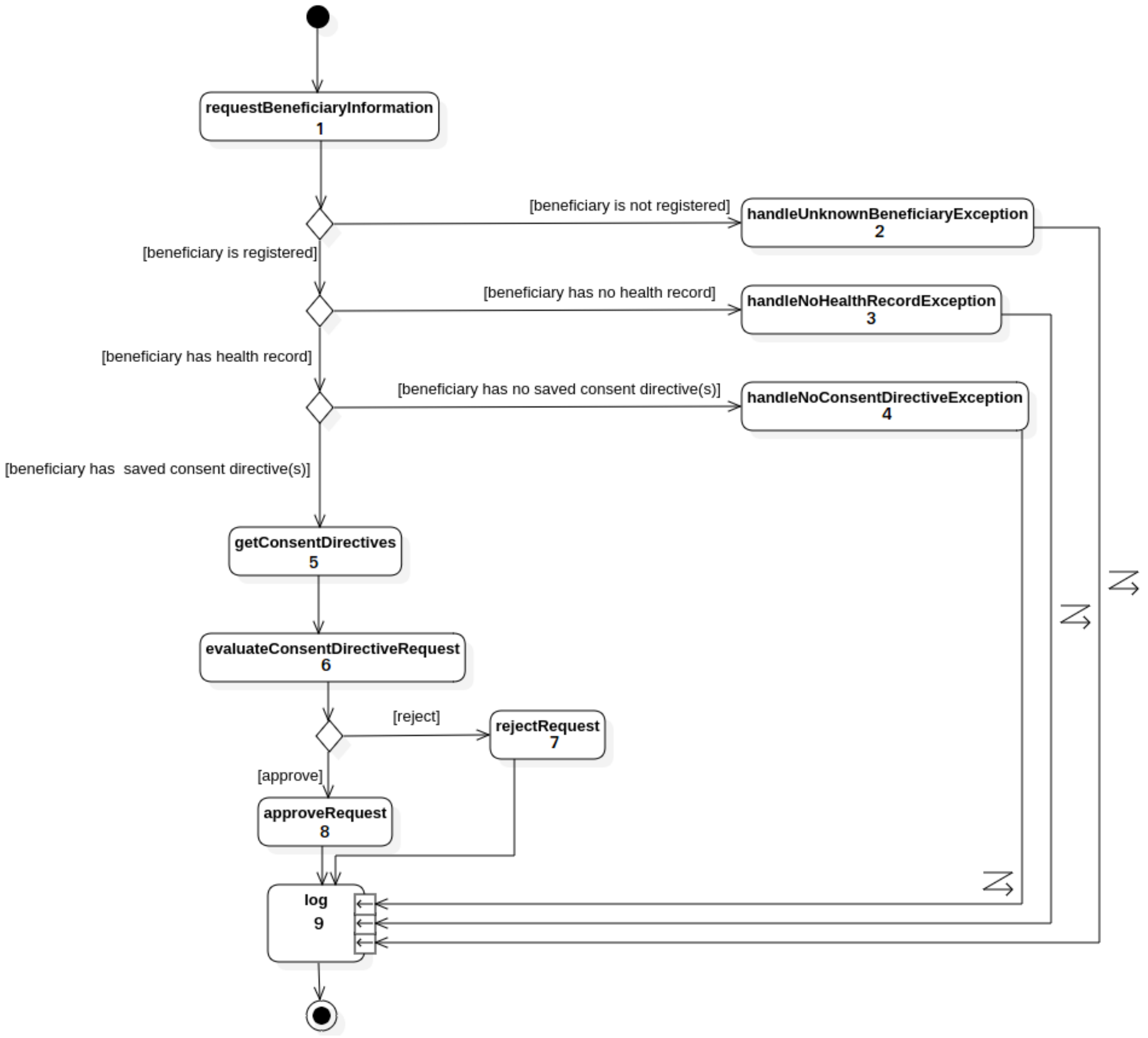

requestBeneficiaryInformation
1
[beneficiary is not registered]
handleUnknownBeneficiaryException
2
[beneficiary is registered]
[beneficiary has no health record]
handleNoHealthRecordException
3
[beneficiary has health record]
[beneficiary has no saved consent directive(s)]
handleNoConsentDirectiveException
4
[beneficiary has saved consent directive(s)]
getConsentDirectives
5
evaluateConsentDirectiveRequest
6
[reject]
rejectRequest
7
[approve]
approveRequest
8
log
9

Figure 4.10: Process of requesting beneficiary information

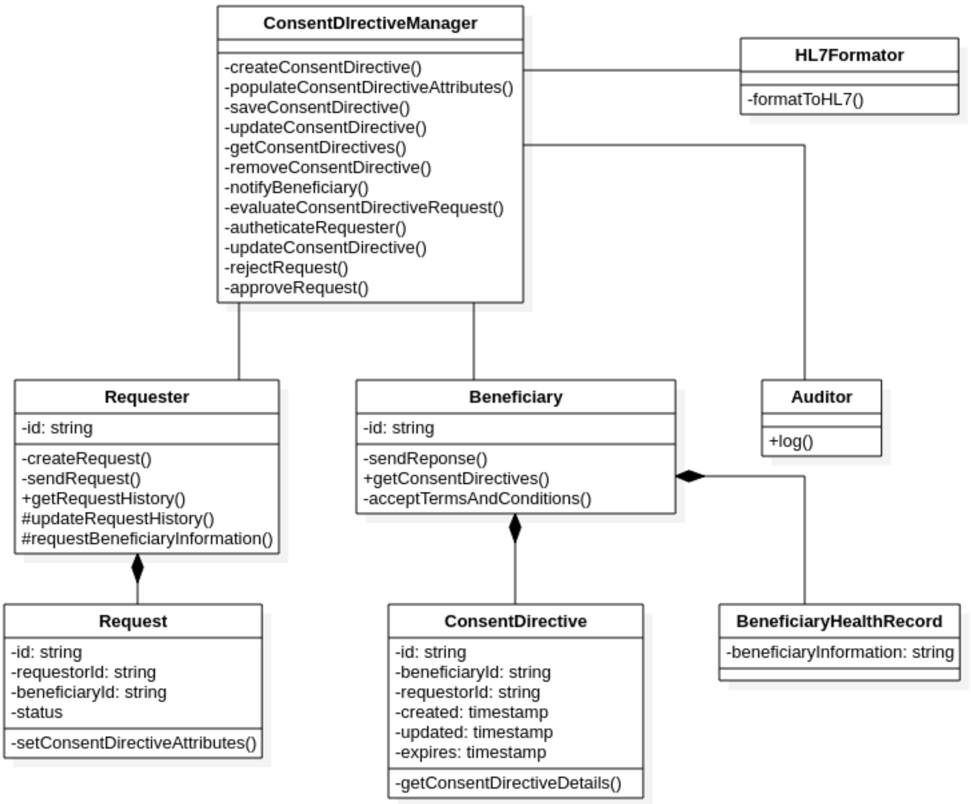


Figure 4.11: e-Consent management system architecture

The consent directive manager begins by checking if Jane exists on the HIS, and whether or not she has both a consent directive and an electronic health record **(1)**. When all three conditions are fulfilled **(2-4)**, the consent directive manager proceeds to retrieve the consent directive **(5)** and evaluates the request against the conditions stipulated in the consent directive **(6)**. Based on the evaluation result, the request is either rejected **(7)** or approved **(8)**. The transaction is then logged, and the process terminates **(9)**.

4.4 Summary

This chapter presented the first contribution chapter of this paper, which is an e-consent management system model. The requirements the e-consent management system should satisfy were explained and the relationship between the security, privacy and consent dimensions were illustrated.

The chapter also illustrated design diagrams that show the components of the system, as well as the flow of the processes when the components interact with each other. The next chapter presents the third contribution of this research which is the e-consent management system prototype.

Chapter 5

e-Consent Management System Prototype Implementation

5.1 Introduction

This chapter presents the prototype of the proposed e-Consent Management System (eCMS). The prototype is implemented based on the model and the architectural design developed in Chapter 4.

Through the application of the principles and guidelines across the regulations and laws mentioned in this research, a software system, which protects the privacy rights of beneficiaries, can be developed. The remainder of this chapter is structured as follows: Section 5.2 describes the technologies used to implement the eCMS, how the application is made available to its users and the implementation details of the application's functionality. The chapter concludes with a summary in Section 5.3.

5.2 The eCMS Implementation Details

The eCMS is a web application designed to be accessible to online beneficiaries and healthcare professionals for consent directive management. The application was developed using Node.js (Version 8.10.0), which is an open-source JavaScript runtime environment that can execute JavaScript code outside the browser [71]. Node.js is lightweight, asynchronous and runs on Windows, MAC and Linux [71]. Node.js was used to create a scalable RESTful API, which utilises HTTP requests to GET, POST, PUT, PATCH and DELETE data [14] for eCMS. The database management system chosen for eCMS is PostgreSQL (Version 12.0), which handles the storage, retrieval and manipulation of data in the database. PostgreSQL is open-source and integrates easily with Node.js [88].

The eCMS was developed on Ubuntu 16.04.5 and tested in Linux and Windows environments. The application is accessible via a URL without the need for installation.

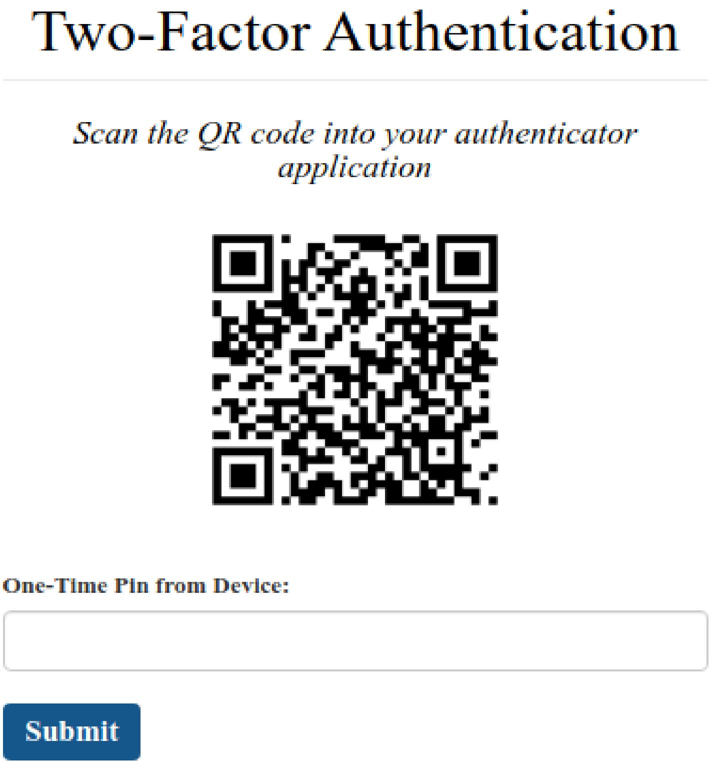
The rest of this section discusses how aspects of the system such as security, informativity, controllability, modifiability and privacy, were implemented. These aspects originate from the model developed in Chapter 4 in order to guide the implementation of a secure consent management system. In the subsequent sections, the mechanisms for each of the aspects are discussed in detail.

5.2.1 Implementing Security for the eCMS

This section discusses the security mechanisms to implement security services, such as identification and authentication, access control, confidentiality and integrity.

5.2.1.1 User Identification and Authentication

During the login process, each user is required to enter his/her username and password, followed by a timed one-time pin (TOTP). The two-factor authentication procedure ensures a more secure user identification and authentication process. When the user logs into the eCMS for the first time, he/she is required to register for two-factor authentication by scanning the QR code from the eCMS on an authentication application as illustrated in Figure 5.1.



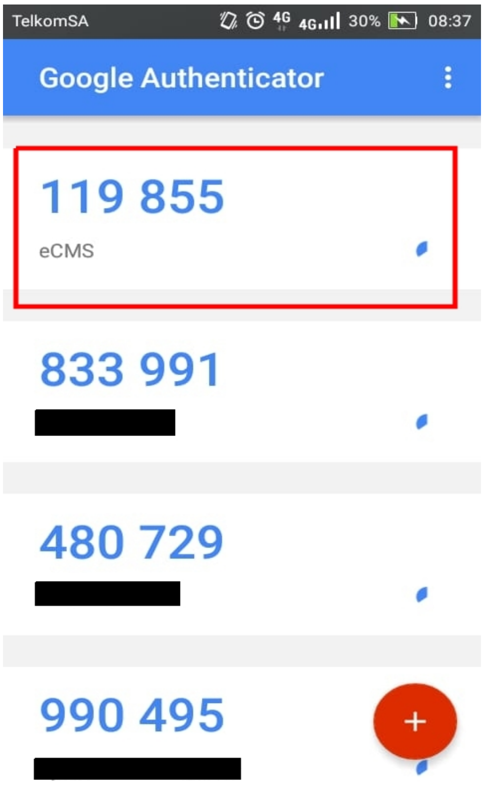
Two-Factor Authentication

Scan the QR code into your authenticator application

Figure 5.1: Two-factor authentication registration on eCMS

Authentication applications such as Google Authenticator generate TOTPs that a user enters into the eCMS during subsequent logins. Google Authenticator can be installed on Android, BlackBerry, and iOS devices. On the eCMS application, a new user is presented with a QR code as shown in Figure 5.1. When the user scans the QR code on the Google Authenticator application, the eCMS is stored as an entry and a new TOTP for the eCMS is generated every 30 seconds, as illustrated in Figure 5.2.

When a new user enters the TOTP he/she is successfully registered and a base32 secret key associated with the user is stored in the eCMS database. Base32 is an encoding scheme comprising 26 uppercase letters A to Z and the numbers 2 to 7 [56], e.g. "PIZDGZLEMY3XS2BZNI4TSNDE".



TelkomSA 4G 4G 30% 08:37

Google Authenticator

119 855

eCMS

833 991

[redacted]

480 729

[redacted]

990 495

[redacted]

Figure 5.2: The TOPT on the Google Authenticator mobile application

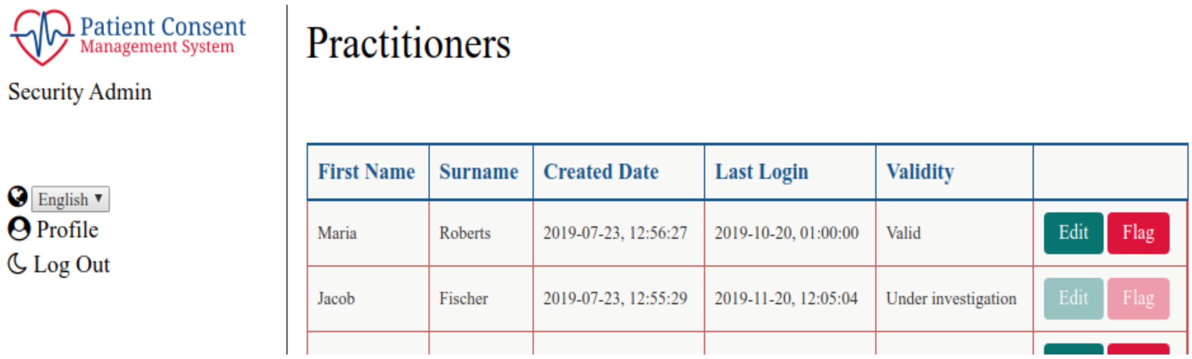
Once the user has logged in, he/she gains access to eCMS functionality based on his/her user role and privileges. The next section discusses how access control is approached in the system.

5.2.1.2 Access Control

The eCMS accommodates four user roles: the beneficiary, the provider, the system administrator and the security administrator. Beneficiaries include any healthcare user, such as inpatients, outpatients, day patients, pharmaceutical users or any other consumer of healthcare. Providers include doctors, nurses, pharmacists, researchers or any other worker in the healthcare field.

The function of the system administrator is limited to account management and moderating the functionality each user may have access to. The system administrator and security administrator do not have access to the personal health information of the beneficiaries. The role of the security administrator is to review the audit logs of the system so that any malicious behaviour can be identified.

The list of healthcare professionals that are available on the system are valid practitioners who are authentic and active members of the medical profession. Valid practitioners include those who are not retired, are not under investigation, and have a medical practitioner registration number. Healthcare professionals who are invalid are flagged by the security administrator and can no longer access the eCMS as illustrated in Figure 5.3. Additionally, the system automatically deactivates all consent directives associated with the healthcare professional so that he/she can no longer access beneficiary information. A healthcare professional's access is revoked when he/she is found to have violated the policy of code or conduct of his/her place of employment or when he/she is reported by the security administrator after the detection of malicious activity.



Practitioners

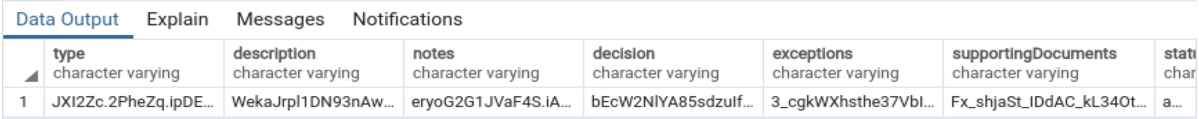
First Name	Surname	Created Date	Last Login	Validity	
Maria	Roberts	2019-07-23, 12:56:27	2019-10-20, 01:00:00	Valid	Edit Flag
Jacob	Fischer	2019-07-23, 12:55:29	2019-11-20, 12:05:04	Under investigation	Edit Flag

Figure 5.3: Flagged users by security administrator

The next section discusses the information security mechanisms used to enforce information integrity and to ensure user accountability in the eCMS. Given the sensitive nature of the eCMS information, it is integral that the integrity and confidentiality of its information are maintained as undue disclosure may violate the privacy rights of its users.

5.2.1.3 Information Confidentiality and Integrity

The eCMS information, such as beneficiary details and consent directives, are stored in the database an encrypted state. Storing information in an encrypted state ensures that information is not readily readable, especially when it is obtained by attackers. Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) is used in the eCMS for encryption. Given that encryption does not ensure the integrity of information, techniques such as hash-based checksums are usually performed to verify that information was not modified. For this reason, using AES would not satisfy the integrity requirement for the system. AES-GCM is used as it provides both encryption and authenticity measures by maintaining confidentiality and integrity. Figure 5.4 illustrates a snippet of encrypted data in the eCMS consent directive table.



	type character varying	description character varying	notes character varying	decision character varying	exceptions character varying	supportingDocuments character varying	statı char
1	JXI2Zc.2PheZq.ipDE...	WekaJrpl1DN93nAw...	eryoG2G1JVaF4S.iA...	bEcW2NlYA85sdzulf...	3_cgkWXhsthe37Vbl...	Fx_shjaSt_IDdAC_kL34Ot...	a...

Figure 5.4: PostgreSQL consent directives table with encrypted data

Mechanisms have been put in place to trace parties involved in violating the rights of a beneficiary on the eCMS by a user in the event of this occurring, so that the user may be held accountable. The next section discusses the mechanisms to support accountability.

5.2.1.4 Accountability

This section discusses how the Audit Trail and Node Authentication (ATNA) Integration Profile and blockchain technology are used to maintain accountability on the eCMS.

ATNA Integration Profile for an Audit Trail

Auditing is conducted in the system using the ATNA Integration Profile which is a part of the Integrated Health Exchange (IHE) IT infrastructure technical framework. The function of the IHE technical framework is to improve the way HISs communicate with each other by using standards that promote interoperability [73]. ATNA provides a standardised and flexible infrastructure to gather audit information [16]. It is used to log actions are performed on a patient's health information, security and user authentication [7].

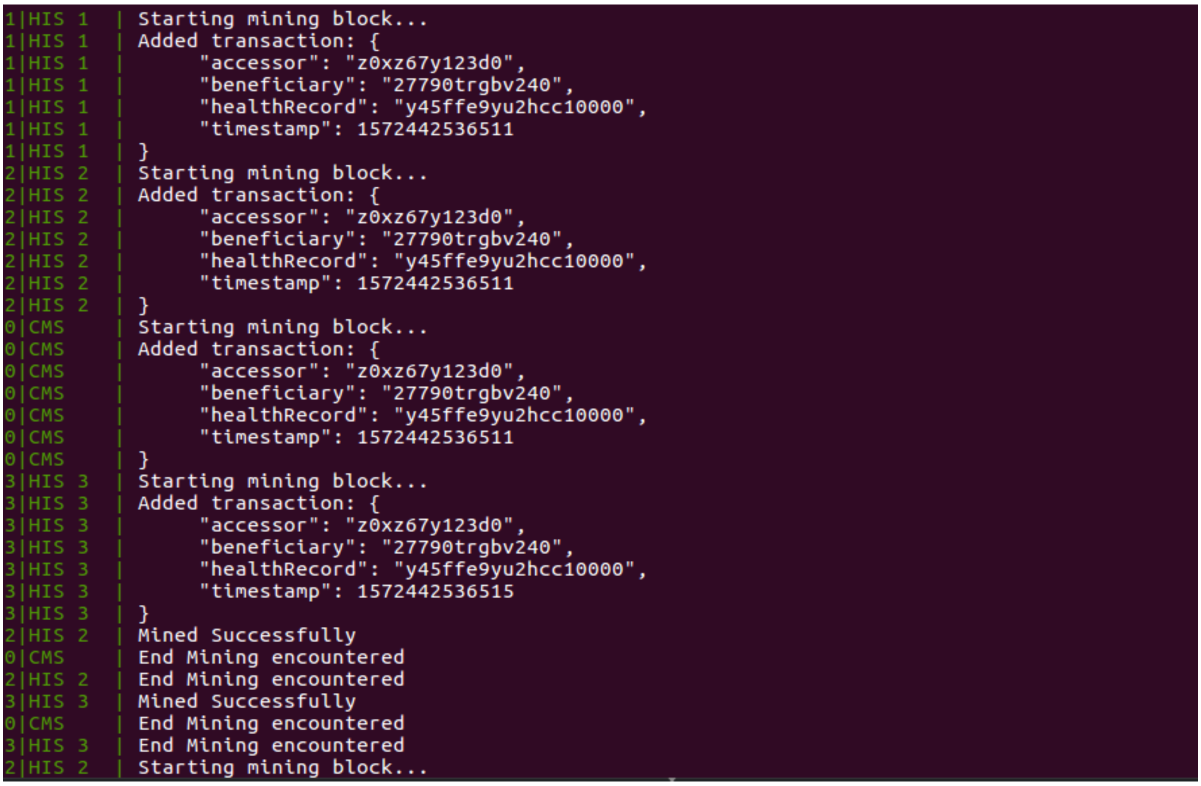
When the eCMS node interacts with other HIS nodes, each node is expected to be secure and to use secure information. Audit logs are an important aspect of the eCMS when the security of the nodes is threatened, as they give a detailed trace of actions by providing timelines that include information such as machine identities, IP addresses and logged in users etc. Using the audit log information, the security administrator can gather evidence to use against a suspicious user during a case.

In regulations such as GDPR, it is specified that regular auditing needs to be conducted to prove that the level of security is at its best [61]

Blockchain for Accountability

Blockchain technology is used in the eCMS to track and verify transactions between HISs that involve the medical record information of the beneficiary. It is an additional layer for the integrity and accountability of the eCMS. A blockchain is a series of connected data structures called blocks that record information across a distributed system where each block depends on the previous block [60].

The benefit of blockchain is that it makes it difficult to corrupt information. Blockchain contains immutable cryptographically verifiable data and validates the data before it adds it to the chain [32, 60]. During a forensics process, a blockchain can be used as evidence as it provides provenance and traceability due to its immutable nature. Information included in each block includes hashes of the directive, health records as well as information regarding the nature of the transaction and the parties involved. Figure 5.5 illustrates a mining process in which HIS1 adds a transaction to the blockchain and all the other nodes (i.e HIS2, HIS3 and eCMS) update their transactions with the latest transaction.



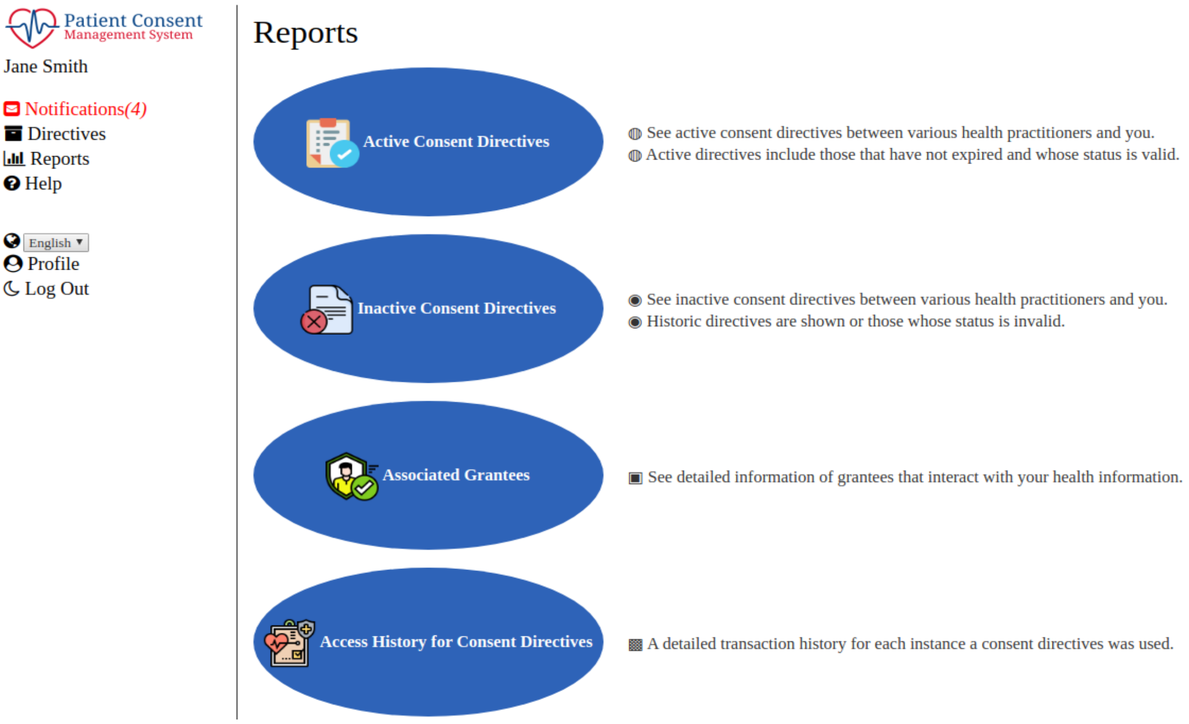
```
1|HIS 1   | Starting mining block...
1|HIS 1   | Added transaction: {
1|HIS 1   |     "accessor": "z0xz67y123d0",
1|HIS 1   |     "beneficiary": "27790trgbv240",
1|HIS 1   |     "healthRecord": "y45ffe9yu2hcc10000",
1|HIS 1   |     "timestamp": 1572442536511
1|HIS 1   | }
2|HIS 2   | Starting mining block...
2|HIS 2   | Added transaction: {
2|HIS 2   |     "accessor": "z0xz67y123d0",
2|HIS 2   |     "beneficiary": "27790trgbv240",
2|HIS 2   |     "healthRecord": "y45ffe9yu2hcc10000",
2|HIS 2   |     "timestamp": 1572442536511
2|HIS 2   | }
0|CMS     | Starting mining block...
0|CMS     | Added transaction: {
0|CMS     |     "accessor": "z0xz67y123d0",
0|CMS     |     "beneficiary": "27790trgbv240",
0|CMS     |     "healthRecord": "y45ffe9yu2hcc10000",
0|CMS     |     "timestamp": 1572442536511
0|CMS     | }
3|HIS 3   | Starting mining block...
3|HIS 3   | Added transaction: {
3|HIS 3   |     "accessor": "z0xz67y123d0",
3|HIS 3   |     "beneficiary": "27790trgbv240",
3|HIS 3   |     "healthRecord": "y45ffe9yu2hcc10000",
3|HIS 3   |     "timestamp": 1572442536515
3|HIS 3   | }
2|HIS 2   | Mined Successfully
0|CMS     | End Mining encountered
2|HIS 2   | End Mining encountered
3|HIS 3   | Mined Successfully
0|CMS     | End Mining encountered
3|HIS 3   | End Mining encountered
2|HIS 2   | Starting mining block...
```

Figure 5.5: Blockchain mining between HISs simulation

This section concludes the security aspects for the eCMS. The following section discusses how informativity was achieved in the system to ensure that the beneficiary is equipped with the knowledge to make informed decisions and is aware of activities related to his/her information.

5.2.2 Implementing Informativity for the eCMS

The beneficiary is provided with relevant and qualitative information so that he/she can give his/her informed consent. The eCMS facilitates informed consent by providing media from the practitioner, which details more in-depth information that may assist the beneficiary in making a decision. Additionally, the beneficiary is provided with an avenue to easily ask questions that relate to his/her consent directive. The beneficiary is notified about any changes requested by the service provider for his/her consent directives. The eCMS also provides reports that detail requests that were made using his/her consent directives and the grantees involved, as illustrated in Figure 5.6. At the end of each year, an automated report is sent to the beneficiary summarising all transactions related to his/her personal information.



◍ See active consent directives between various health practitioners and you.
◍ Active directives include those that have not expired and whose status is valid.

◉ See inactive consent directives between various health practitioners and you.
◉ Historic directives are shown or those whose status is invalid.

▣ See detailed information of grantees that interact with your health information.

▩ A detailed transaction history for each instance a consent directives was used.

Figure 5.6: Reports available for the beneficiary

The following section discusses how user controllability was implemented in the eCMS so that the beneficiary can oversee and make decisions related to his/her information.

5.2.3 Implementing Controllability for the eCMS

The beneficiary is provided with the means to easily give or revoke his/her consent given to a service provider. Specifically, a beneficiary can give a decision to provide *no consent*, *opt in*, *opt in with exceptions*, *opt out* or *opt out with exceptions* for a consent directive. In the event the beneficiary is suspicious of the activity that relates to the access of his/her medical information, he/she is able to flag the behaviour to the appropriate party. Transparency between the beneficiary and the HISs fosters trust and eventually aids research endeavours so that more beneficiaries participate in studies by giving more access to their information. Highly quantitative and qualitative access to information allows for improved medical studies as it reduces research time and produces superior output.

The following section discusses how modifiability was implemented in the eCMS in order to facilitate flexibility for the beneficiary.

5.2.4 Implementing Modifiability for the eCMS

The beneficiary is provided with the means to easily modify his/her consent directives after he/she has given informed consent. In the event a beneficiary wishes to modify attributes of the directive, such as the timespan or the grantee, a request can be sent through the eCMS. The functionality for informativity, controllability and modifiability are illustrated in detail in the following chapter.

The following section discusses how the principles of the PoPIA were integrated into the eCMS to follow a privacy-driven implementation process.

5.2.5 Applying PoPIA Principles for a Privacy-Driven Design

Privacy by Design (PbD) is a concept developed to promote privacy and data protection in information technology and communication systems. The GDPR advocates for stronger personal data protection and. Under the GDPR, it is mandatory for a PbD approach to be followed, as it anticipates and prevents privacy issues even before a software system is created [61].

PbD comprises seven principles that propose the adoption for a privacy-driven design approach. The PbD principles [22, 74] are described in more detail below:

- *Proactive not reactive:* PbD should anticipate privacy risks and prevent them from materialising.
- *Privacy as the default setting:* Personal data should automatically be protected by default with no added action required from the user.
- *Privacy embedded into the design:* Privacy measures should be embedded into the architecture and design of IT systems as the integral component.
- *Full functionality:* PbD should ensure that even though privacy is the core objective, it does not impair other functionalities of the system.
- *End-to-end security:* Confidentiality should be continuously enforced across the entire lifecycle of the data. Without strong security, confidentiality cannot be realised.
- *Visibility and transparency:* All stakeholders should operate according to the stated promises.
- *Respect for user privacy:* A user-centric approach should be undertaken so that users can control their data. This involves requesting consent from the user and ensuring that the users have access to activities surrounding their information.

Table 5.1 illustrates how the PoPIA principles and system requirements identified in Chapter 4, Section 4.2.2 (informativity, modifiability, controllability and security) are aligned to meet the PbD principles. For each PbD principle, there are mechanisms

Table 5.1: Enforcing PoPIA principles to achieve privacy by design for eCMS

PbD Principle	**PoPIA Principle**	**System Requirement**
Proactive not reactive	Security safeguards	Security
Privacy as the default setting	Accountability, Processing limitation, Purpose specification, Further-processing limitation	Security
Privacy embedded into the design	Security safeguards	Informativity, Security
Full functionality		Informativity, Modifiability, Controllability Security
End-to-end security	Security safeguards	Security
Visibility and transparency	Accountability, Openness, Data subject participation	Informativity, Modifiability, Controllability
Respect for user privacy	Information quality, Data subject participation	Informativity, Security

to achieve the system requirements to ensure the eCMS privacy preserving application. For instance, in order to achieve the *proactive and not reactive* principle and meet the PoPIA *security safeguards*, the eCMS security aspects are applied.

Embracing beneficiary privacy can promote the stream of information as patients are encouraged to participate in research. When beneficiaries do not know who exactly is accessing their information and the purpose for which it is being accessed, they are less willing to share their information [106]. In order to address these privacy concerns, a channel for providing consent needs to be developed to verify that directives are being followed.

When an effective consent process is followed, it ensures the following [106]:

- Improved research participation.
- Increased access to beneficiary data and biological specimens.
- Reduced cost and time for recruiting beneficiaries for clinical trials.
- Accelerated creation of new treatments.

In order to take advantage of the information that resides in the eCMS database, machine learning is applied to aid the medical research process. The details of the approach used are discussed in the following section.

5.2.6 Research Assistance

Most participants (91%) in a medical research study would be partial to opting in before their personal identifiable information can be used [95]. It is important to attract the trust of beneficiaries as it enables researchers, medical practitioners and scientists to have access to beneficiary EHRs. The purpose of the EHR is firstly to assist the medical team in recalling and communicating the health and treatment of a beneficiary in a coherent manner. Secondly, an EHR is an origin of statistical information on the variety of beneficiaries and the outcomes of their respective treatments [3].

In order to assist the research process, machine learning capabilities can be applied. An Artificial Neural Network (ANN) for the eCMS is trained using data within the management system database. Once trained, the ANN gives the likelihood of the viability of suitable beneficiary candidates.

The scientist or researcher is notified of beneficiaries who are more likely to accept the conditions of a consent directive within a certain time frame. Inputs that are used to train the ANN include the reaction time of the beneficiary, type of directive and the response.

5.2.6.1 Generating Training Data

The training data was obtained from simulated beneficiary profiles on the eCMS. The training data comprised four attributes: how quickly the beneficiary responds to directives (short or long), how many requests the beneficiary has approved before in relation to the total number of requests they have received in the past (low or high), if they have specifically excluded any practitioners or facilities (1 represents true and 0 represents false), and whether the beneficiary is acceptable based on the previous three attributes. The viability of a beneficiary can be represented in a truth table as illustrated in Table 5.2.

Table 5.2: Neutral Network Truth Table

Input 1	**Input 2**	**Input 3**	**Output**
short	high	1	1
short	high	0	1
short	low	1	0
short	low	0	0
long	high	1	0
long	high	0	1
long	low	1	0
long	low	0	0

Each attribute is normalised such that (i) $0 \leq input1 < 1.4$, (ii) $\{input2 \in \mathbb{Q} | 0 \leq input2 < 1\}$, (iii) $input3 \in [0, 1]$ and (iv) $output \in [0, 1]$.

5.2.6.2 Training the Neutral Network

The ANN was developed using an input layer (i), a hidden layer (j) with six nodes and an output layer (k). The ANN uses a feed-forward network where the inputs are received and activated, and the output (y) serves as input to the next layer. The structure of the ANN is illustrated in Figure 5.7.

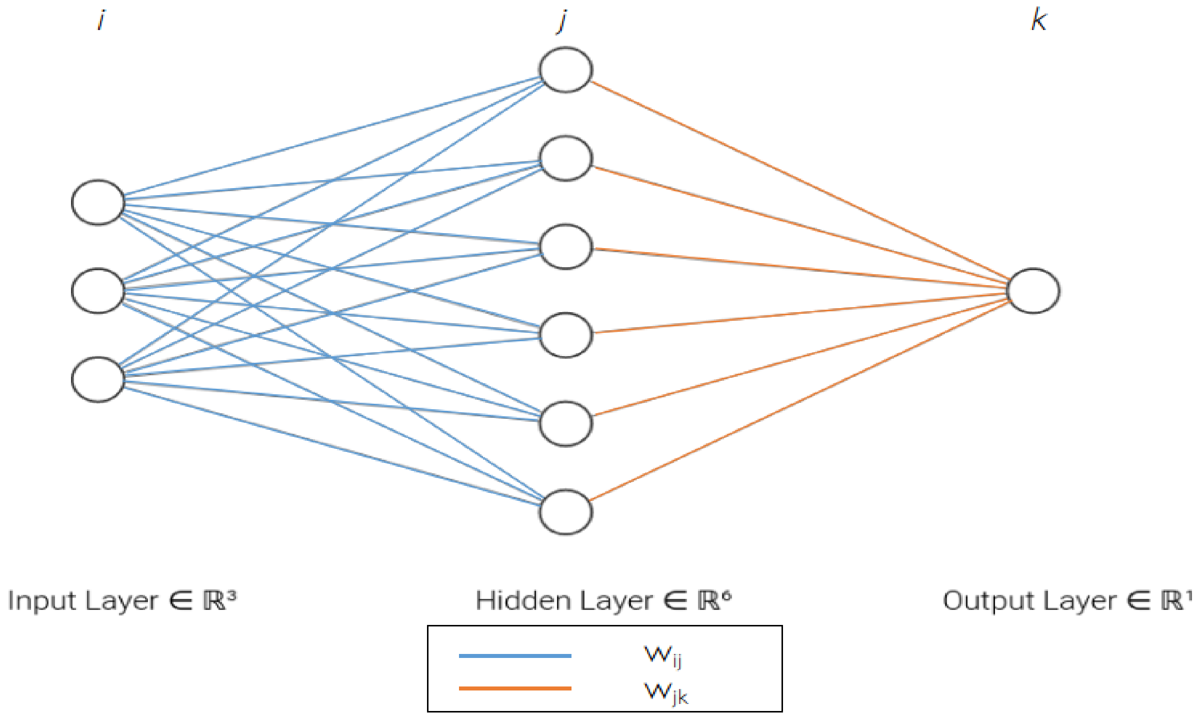


Figure 5.7: The ANN structure

The activation function, which is the mechanism to get output from the ANN node, is the hyperbolic tangent activation function (also known as tanh). It is mainly used to distinguish between two categories, expressed in Equation 5.1 as follows:

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{5.1}$$

The algorithm (Equation 5.2) that the ANN uses to learn is called backpropagation and it teaches the ANN what the correct output should be for a specified input. The learning rate (ε) selected for the ANN is 0.3.

$$\Delta w_{ab} = \varepsilon \frac{\partial E_b}{\partial w_{ab}} \tag{5.2}$$

The ANN learns by adjusting its weights, starting from the output layer and moving backwards so that when the same input is fed into the ANN, a more accurate output is produced. The derivative of the activation function is expressed in Equation 5.3. It uses a gradient descent calculation, which adjusts the weights of the ANN.

$$\frac{d}{dx}tanh(x) = 1 - \frac{(e^x - e^{-x})^2}{(e^x + e^{-x})^2} = 1 - tanh^2(x) \tag{5.3}$$

The delta rule calculates the gradient and adjusts the weights of the ANN during back-propagation. For each layer, the delta (δ) is calculated as shown in Equation 5.4.

$$\delta_b = E_b.f'(\sum_b w_{ab}.y_b) \tag{5.4}$$

Firstly, the error of the output layer is calculated by calculating the difference between the ANN output and the expected output as shown in Equation 5.5.

$$E_k = expected - y_k \tag{5.5}$$

Next, the delta of the output layer (δ_k) is calculated using Equation 5.4 where the error is multiplied by the derivative of the sum of inputs from the hidden layer. At the hidden layer, the error for the layer is calculated as shown in Equation 5.6, where δ_k is multiplied by each weight between the hidden and output layer.

$$E_j = \sum \delta_j.w_{jk} \tag{5.6}$$

The new weights between the output and the hidden layer are then updated using the backpropagation formula from Equation 5.2. Next, the delta for the hidden layer (δ_j) is calculated using Equation 5.4 and the new weights between the hidden layer and the output layer are updated using Equation 5.2.

For the ANN, about 80% of the input data is used for training and 20% of the data is used for validating. The validation process is discussed in the section that follows.

5.2.6.3 Testing the Neutral Network with Validation Data

Once training for the ANN is completed, the ANN is run with inputs it has not seen before to measure how well it can accurately predict the correct output. It was observed that the error rate of the ANN decreases as the ANN gets trained. as well as when it is validated, as illustrated in Figure 5.8 and Figure 5.9, respectively.

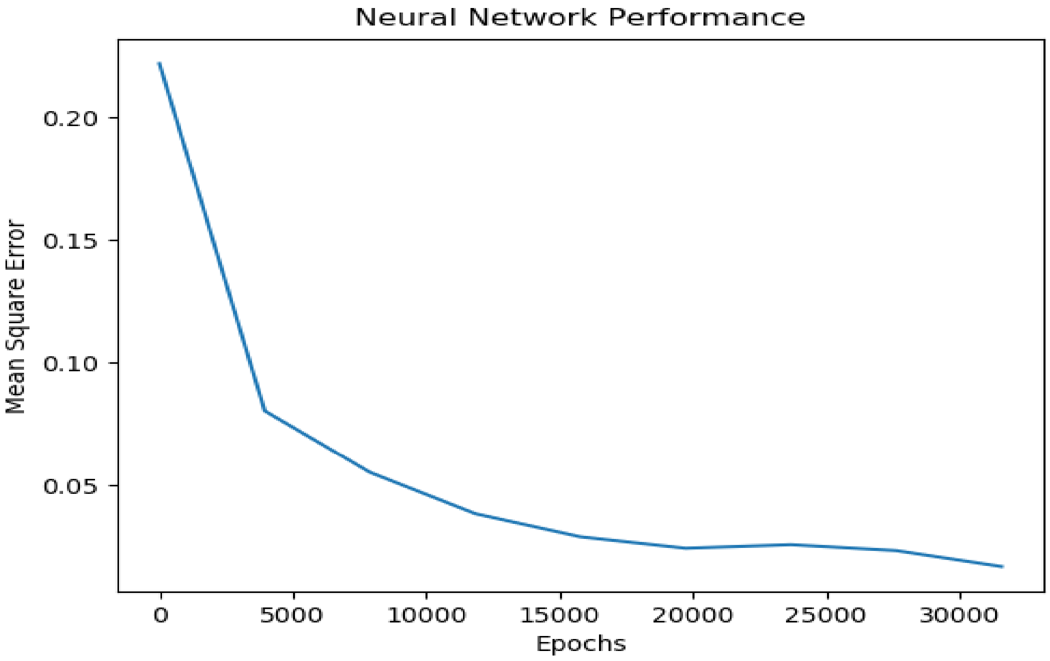


Figure 5.8: Neural Network Performance During Training

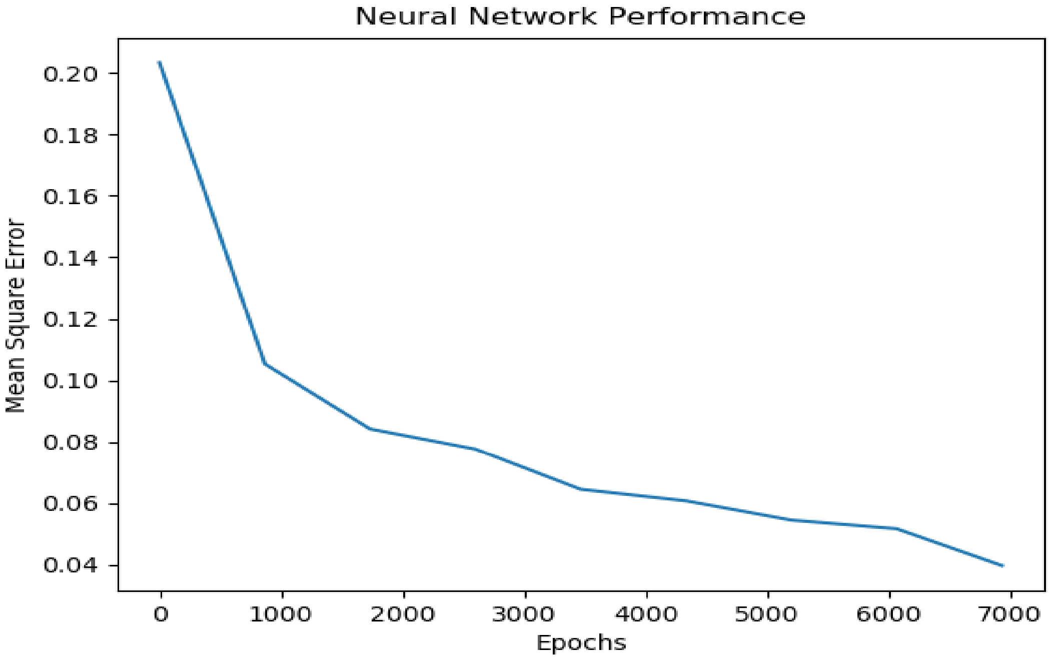


Figure 5.9: Neural Network Performance During Validation

As the number of iterations for the neural network increases, the error rate decreases, which is the desirable ANN performance.

5.3 Summary

This chapter presented the eCMS prototype that was developed based on the model and the architectural design developed in Chapter 4. The system provides reporting functionality, as well as research assistance by way of a neural network. By applying the informativity, modifiability, controllability and security requirements of the system, a privacy preserving eCMS was developed. The following chapter demonstrates the consent directive life cycle by way of a fictional case scenario.

Chapter 6

e-Consent Management System Prototype Demonstration

6.1 Introduction

This chapter presents the functionality of the eCMS prototype by way of a scenario. The workflows for each aspect of the consent directive life cycle in the eCMS are detailed. Sections 6.2 to 6.5 demonstrate the functions of the prototype in which consent directives are created, retrieved, updated and removed, respectively. The chapter concludes with a summary in Section 6.6

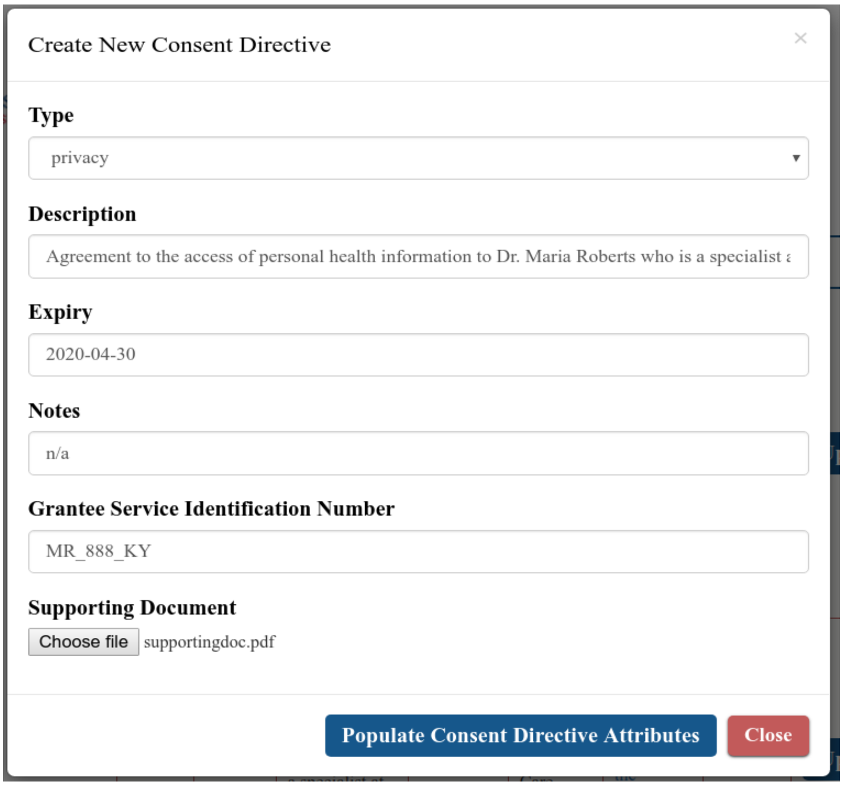
6.2 Consent Directive Creation

This section illustrates how the scenario in Chapter 4, Section 4.3.3.1.1 (in which the consent directive creation workflow via UML is described) is demonstrated in the system. In the scenario, Dr Fischer creates a new directive for Jane so that Dr Roberts may have access to Jane's medical history.

In Figure 6.1, Dr Fischer specifies the consent attributes for the directive. This includes the directive type ("privacy"), description ("Agreement to provide of personal health information to Dr Maria Roberts who is a specialist at the Centre for Renal Care in Pretoria, South Africa."), expiry ("2020-04-30") and grantee ("Dr Maria Roberts").

Furthermore, Dr Fischer specifies notes related to the directive, as well as any supporting media that can provide Jane with more information so that she can make an informed decision. The supporting media may be a video or a written document that provides a more granular explanation of the description.

Once the request has been sent, the attributes are saved and a notification is sent to both Jane and Dr Fischer informing them of the event. Figure 6.2 shows the directive saved in a "pending_processing" status, while feedback is awaited from Jane. Other statuses for the consent directive include "active" and "inactive". While the consent directive is not in the active state, the grantee will not be able to access the beneficiary's medical information. After the consent directive is created, a notification message is sent to both Jane and Dr Fischer, and the action is logged in the audit logs.



Create New Consent Directive

Type

privacy ▾

Description

Agreement to the access of personal health information to Dr. Maria Roberts who is a specialist a

Expiry

2020-04-30

Notes

n/a

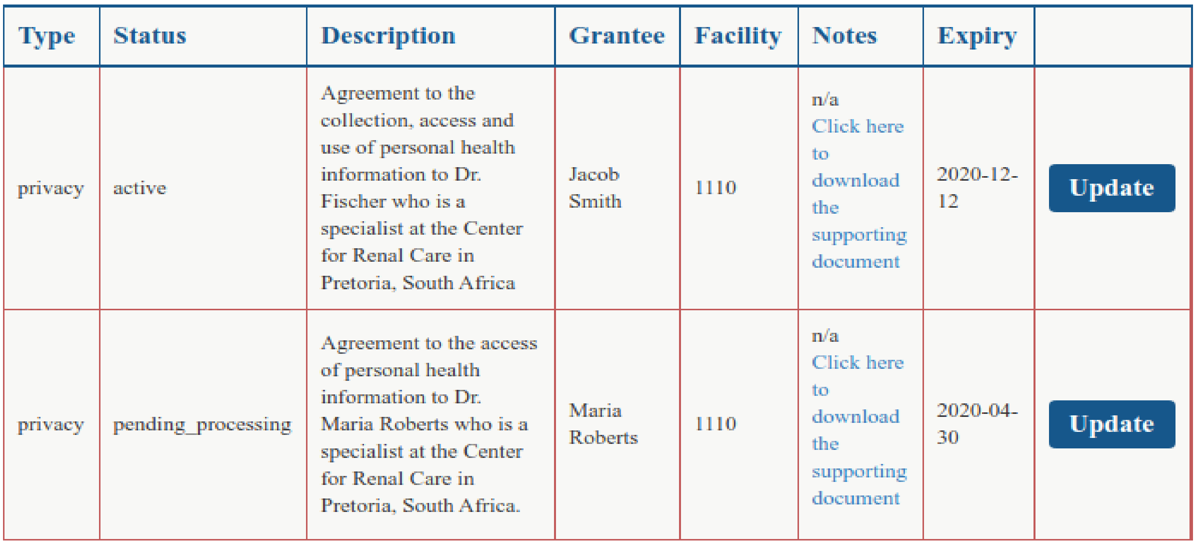
Grantee Service Identification Number

MR_888_KY

Supporting Document

Choose file supportingdoc.pdf

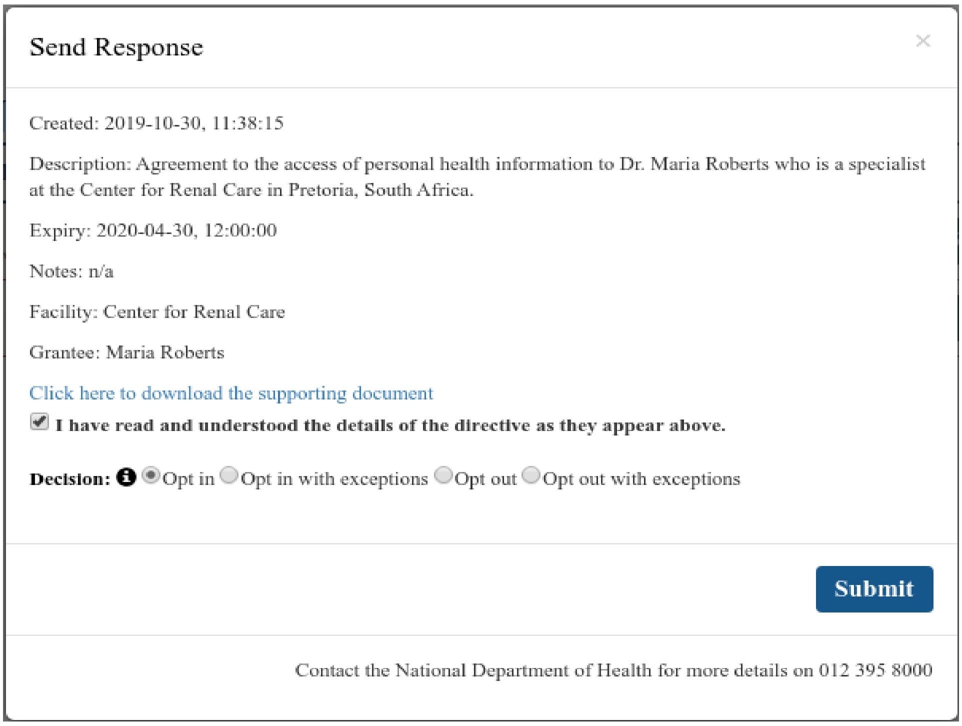
Figure 6.1: Dr. Jacob Fischer creating a new consent directive request for Jane Smith



Type	Status	Description	Grantee	Facility	Notes	Expiry	
privacy	active	Agreement to the collection, access and use of personal health information to Dr. Fischer who is a specialist at the Center for Renal Care in Pretoria, South Africa	Jacob Smith	1110	n/a Click here to download the supporting document	2020-12-12	Update
privacy	pending_processing	Agreement to the access of personal health information to Dr. Maria Roberts who is a specialist at the Center for Renal Care in Pretoria, South Africa.	Maria Roberts	1110	n/a Click here to download the supporting document	2020-04-30	Update

Figure 6.2: The new consent directive is in the "pending_processing" state

In Figure 6.3, Jane sends a response regarding the directive by opting in, having read the supporting media and the purpose specified for the directive. Alternatively, Jane may have chosen to "opt in with exceptions" and may have specified aspects of the directive she did not wish to be included. To confirm Jane's authenticity, she is required to enter a one-time pin before the transaction can be completed. The action is logged in the audit log and a notification is sent to Dr Roberts that the consent directive is now active. Jane's medical information is now available to be accessed by Dr Roberts.



Send Response

Created: 2019-10-30, 11:38:15

Description: Agreement to the access of personal health information to Dr. Maria Roberts who is a specialist at the Center for Renal Care in Pretoria, South Africa.

Expiry: 2020-04-30, 12:00:00

Notes: n/a

Facility: Center for Renal Care

Grantee: Maria Roberts

Click here to download the supporting document

☑ **I have read and understood the details of the directive as they appear above.**

Decision: ℹ ● Opt in ○ Opt in with exceptions ○ Opt out ○ Opt out with exceptions

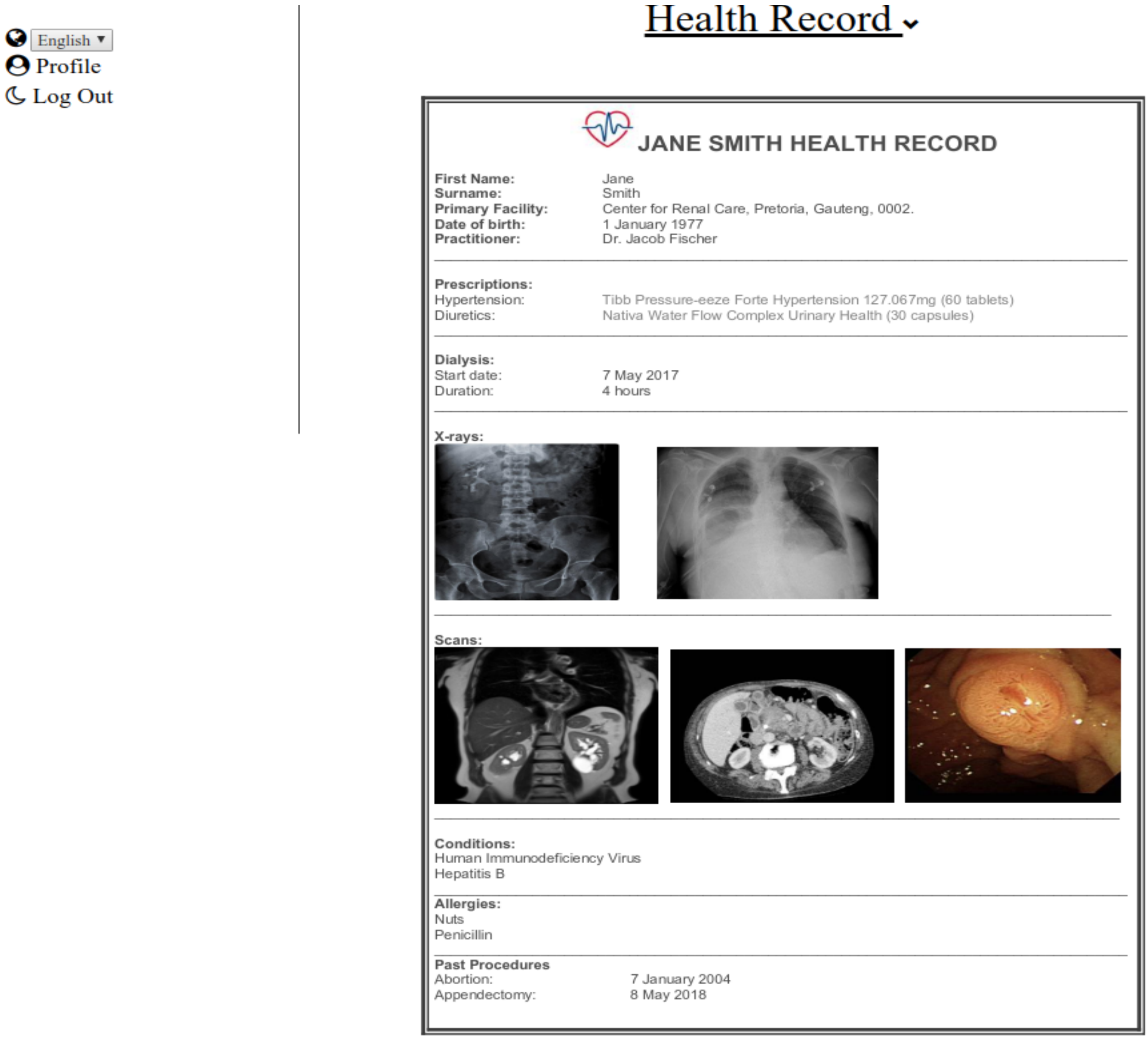
Contact the National Department of Health for more details on 012 395 8000

Figure 6.3: Jane Smith sending a response permitting Dr. Maria Roberts to access information

At each point during the consent directive creation process, an audit trail is formed using ATNA. Furthermore, each time a beneficiary's health record is updated or accessed, the transaction is logged in the blockchain to further enforce accountability and non-repudiation.

6.3 Consent Directive Retrieval

This section illustrates how the scenario in Chapter 4, Section 4.3.3.1.3 (in which the consent directive retrieval workflow via UML is described) is demonstrated in the system. In the scenario, Dr Fischer attempts to view Jane's medical health record as illustrated in Figure 6.4.



JANE SMITH HEALTH RECORD

First Name:	Jane
Surname:	Smith
Primary Facility:	Center for Renal Care, Pretoria, Gauteng, 0002.
Date of birth:	1 January 1977
Practitioner:	Dr. Jacob Fischer

Prescriptions:

Hypertension:	Tibb Pressure-eeze Forte Hypertension 127.067mg (60 tablets)
Diuretics:	Nativa Water Flow Complex Urinary Health (30 capsules)

Dialysis:

Start date:	7 May 2017
Duration:	4 hours

X-rays:

Scans:

Conditions:
Human Immunodeficiency Virus
Hepatitis B

Allergies:
Nuts
Penicillin

Past Procedures

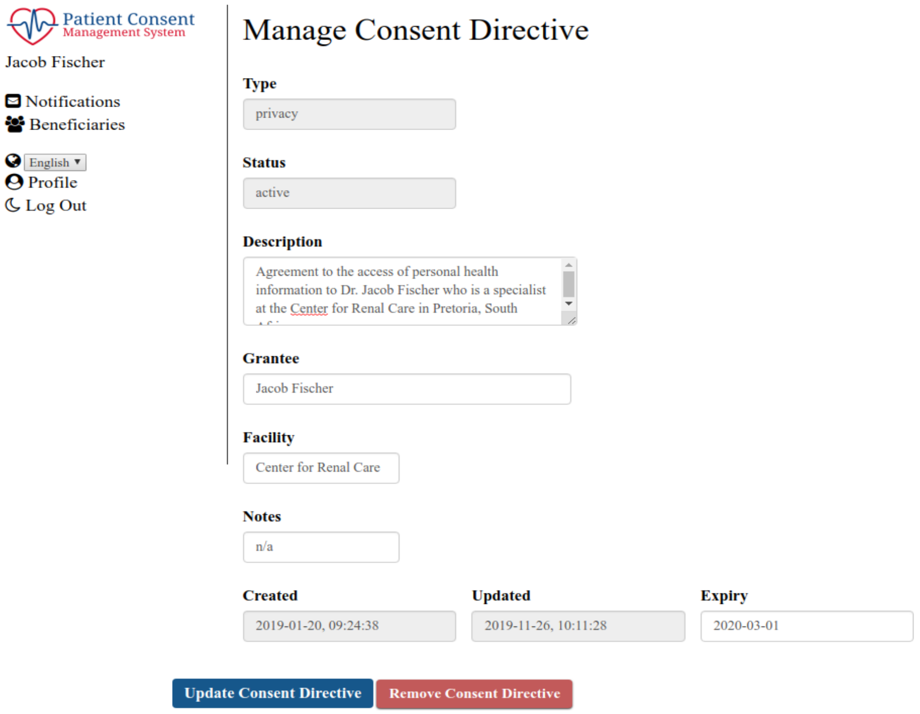
Abortion:	7 January 2004
Appendectomy:	8 May 2018

Figure 6.4: Dr Jacob Fischer retrieves Jane's health record

The eCMS searches for and retrieves the consent directive, the requester and the beneficiary. If the consent directive is active, the doctor's user profile is authorised to view the patient's information.

6.4 Consent Directive Update

This section illustrates how the scenario in Chapter 4, Section 4.3.3.1.4 (in which the consent directive update workflow via UML is described) is demonstrated in the system. In the scenario, Dr Fischer updates Jane's consent directive as illustrated in Figure 6.5.



Manage Consent Directive

Type
privacy

Status
active

Description
Agreement to the access of personal health information to Dr. Jacob Fischer who is a specialist at the Center for Renal Care in Pretoria, South

Grantee
Jacob Fischer

Facility
Center for Renal Care

Notes
n/a

Created	Updated	Expiry
2019-01-20, 09:24:38	2019-11-26, 10:11:28	2020-03-01

Figure 6.5: Dr Maria Roberts retrieves Jane's health record

As the beneficiary, Jane is notified that the directive has been updated and the notifications are visible on a beneficiary dashboard, as illustrated in Figure 6.6.

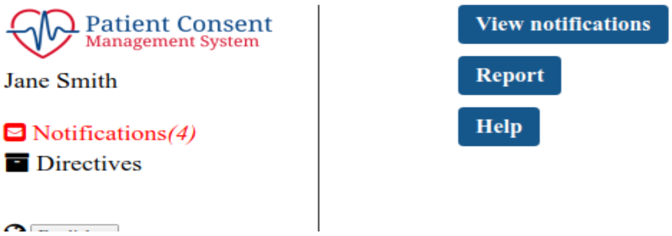
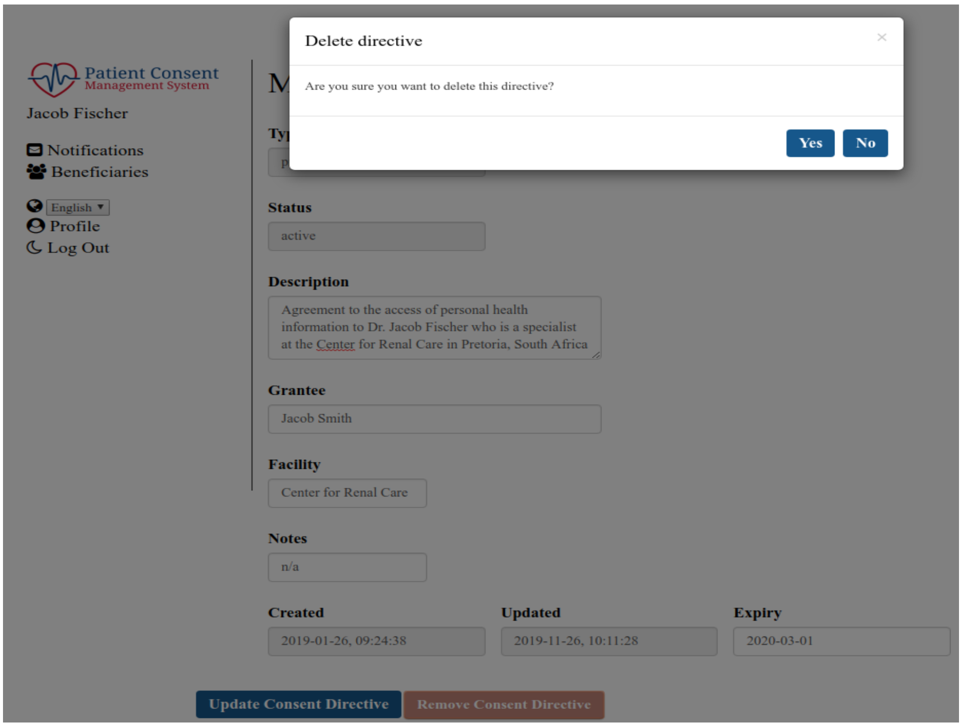


Figure 6.6: Jane is notified that the directive has been updated

6.5 Consent Directive Removal

This section illustrates how the scenario in Chapter 4, Section 4.3.3.1.2 (in which the consent directive removal workflow via UML is described) is demonstrated in the system. In the scenario, Dr Fischer removes a consent directive as illustrated in Figure 6.7 as the reasons for the usage of the directive have expired and are no longer valid. The access is revoked and the practitioner may no longer have access to the information specified in the directive.



Delete directive

Are you sure you want to delete this directive?

Status: active

Description: Agreement to the access of personal health information to Dr. Jacob Fischer who is a specialist at the Center for Renal Care in Pretoria, South Africa

Grantee: Jacob Smith

Facility: Center for Renal Care

Notes: n/a

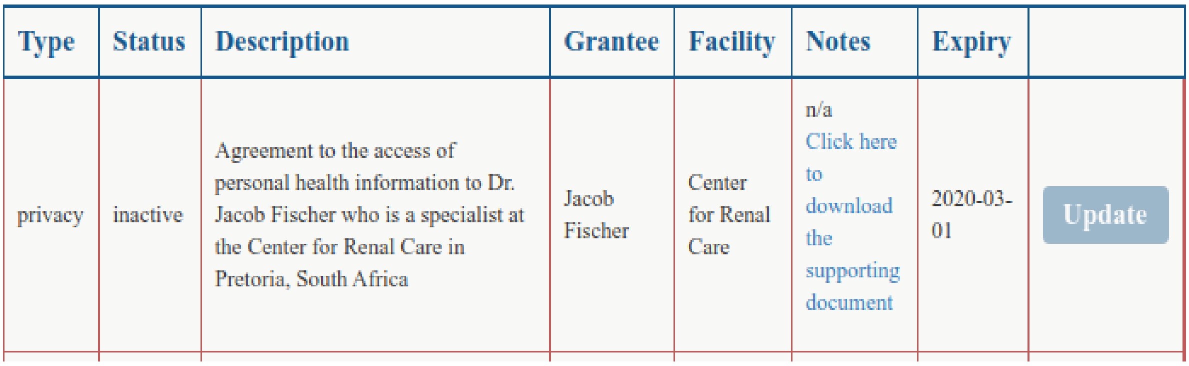
Created: 2019-01-26, 09:24:38

Updated: 2019-11-26, 10:11:28

Expiry: 2020-03-01

Figure 6.7: Dr. Fischer initiates removal process for Jane Smith's directive

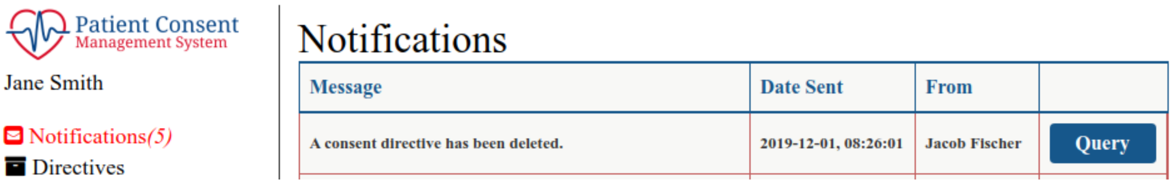
Once Dr Fischer confirms that he wants to continue with the removal workflow the directive is marked "inactive", as illustrated in Figure 6.8.



Type	Status	Description	Grantee	Facility	Notes	Expiry	
privacy	inactive	Agreement to the access of personal health information to Dr. Jacob Fischer who is a specialist at the Center for Renal Care in Pretoria, South Africa	Jacob Fischer	Center for Renal Care	n/a Click here to download the supporting document	2020-03-01	Update

Figure 6.8: Jane Smith's directive with Dr Fischer now has an "inactive" status

Jane is notified that the directive is now inactive and she may send a query regarding the event as shown in Figure 6.9. Other circumstances in which the directive may be marked as inactive are when a practitioner is under investigation or is no longer practising.



Notifications

Message	Date Sent	From	
A consent directive has been deleted.	2019-12-01, 08:26:01	Jacob Fischer	Query

Figure 6.9: Jane Smith is now notified that a consent directive has been removed

6.6 Summary

This chapter demonstrated the system functionality by way of a scenario. The chapter focused on the workflows that are followed during the consent directive life cycle. The following chapter provides an evaluation of the contributions to this research.

Chapter 7

Evaluation

7.1 Introduction

This chapter evaluates the contributions of this research, which include the consent management model, architectural design and prototype. The purpose of the e-consent management system is to give healthcare users control by providing a platform upon which they can make informed decisions. These decisions help healthcare users to control who has access to their personal health information so that unauthorised interactions with the health information are prevented.

The remainder of this chapter is structured as follows: Section 7.2 presents the benefits of the research. Section 7.3 discusses the shortcomings of the research. The chapter concludes in Section 7.4.

7.2 Benefits of the Research

This section discusses the benefits of the research, which include (i) providing easy access for beneficiaries to control their health information, (ii) providing the means for beneficiaries to report behaviours that violate their human rights, (iii) aiding the medical research process by automating search subject selection, and (iv) tracing activities related to beneficiary information and providing immutable evidence for legal action.

7.2.1 Protect the Privacy Rights of Beneficiaries

- The eCMS is designed to ensure that beneficiaries are informed and feel in control of who is accessing their information. The user is informed about who will be accessing his/her information, why the information will be accessed and for which period the authorised access is will be valid.

- Using reports available to the beneficiary and finding that his/her rights were violated, he/she can take his/her grievance to the healthcare provider or to court and provide the information made available by the eCMS.

- The eCMS enforces accountability as each event is logged against a user, so the beneficiary is able to identify the responsible party directly.

7.2.2 Provide Simple Usability and Accessibility

The eCMS achieves Perceived Usefulness (PU) and Perceived Ease of Use (PE). Universal usability is achieved as end-users, independent of which technology they use and their socio-demographic details, can use the system effectively. The three challenges of universal usability (technology variety, user diversity and gaps in user knowledge) [74] are overcome as the system is designed to be information-forward and platform independent.

The system provides functionality to users that is practical and user-friendly, using the following approaches:

- Given that internet connection is expensive for most South Africans [82], the eCMS is designed to use as little bandwidth as possible. When videos are uploaded, the user has the option to download a high quality or a lower quality video in order to accommodate his/her financial bracket, as illustrated in Figure 7.1.

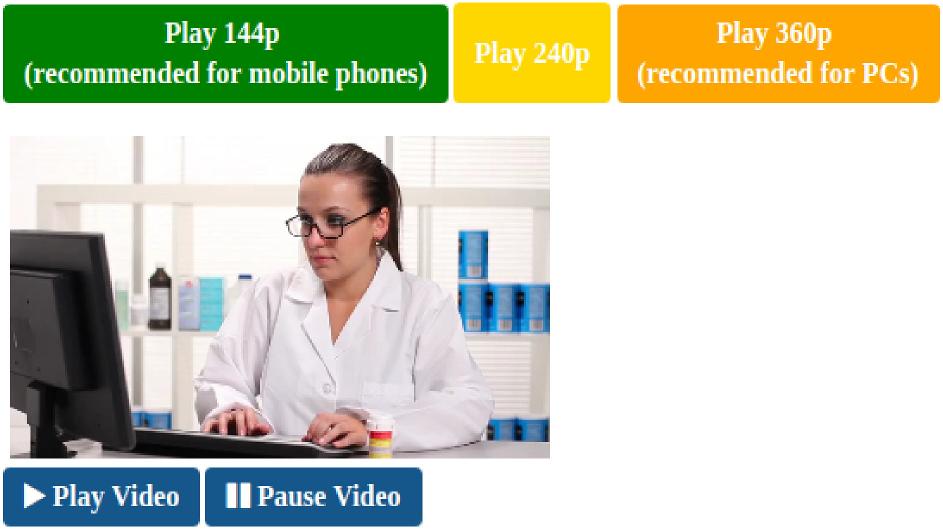


Figure 7.1: Informativity aided by video

Video-assisted informed consent improves the understanding of clinical processes for beneficiaries [59].

- The eCMS is also not device-specific or platform-dependent, it can be used on smart phones, tablets, desktop computers. independent of the device's operating system.

7.2.3 Trace Activities Related to Beneficiary

This section discusses the methods in which activities related to the beneficiary are traced in the eCMS; namely, ATNA auditing and blockchain.

7.2.3.1 ATNA

The ATNA logging was implemented in order to use a standardised and flexible infrastructure to gather audit information. All events related to patient information and general access or use of the system are logged to facilitate accountability. ATNA has a set of functions as described below [8]:

- **User authentication:** Each user must log in to gain access to an HIS in the ATNA environment.
- **Node authentication:** Only authorised nodes in the ATNA environment have access to beneficiary information. ATNA achieves this through the evaluation of digital certificates.
- **Secure communication:** Communication between nodes is encrypted.
- **Audit record generation:** All events are logged and the audit records are sent to an Audit Record Repository. Each record includes the timestamp, enactor, action performed, beneficiary involved and the relevant node(s).

7.2.3.2 Blockchain

Blockchain served as an additional layer of security to facilitate integrity and accountability due to its immutable nature. Blockchain provides provenance and traceability during the forensics process.

7.2.4 Improve Medical Research

Machine learning was implemented using an artificial neural network to help researching doctors to easily identify candidates for medical research processes. The presence of health information systems helps to improve the quality of healthcare [8].

Overall, the benefits satisfy the system requirements for informativity, modifiability, controllability and security, while also maintaining PU and PE. The model, architectural design and prototype are significant contributions. The architectural design and model are novel and well thought through. The prototype implementation successfully proves the concept.

In the next section, the shortcomings of the research are discussed.

7.3 Shortcomings

Some shortcomings of the eCMS are listed below:

- The eCMS relies on online access. The user is required to own a computing device that has access to the internet. In Africa, while an individual is more likely to have access to a cell phone service than piped water, sewage, tarred roads or electricity [85], South Africans from low economic households cannot afford to stay connected to the internet due to the high cost of bandwidth [43].
- The beneficiary needs to have some level of digital literacy and be able to read. South Africans who go to rural schools are less likely to have access to curricula that emphasise computer education. Highly educated beneficiaries are more likely to provide electronic consent [15].
- For good authentication, the beneficiary is required to enter a TOTP using an authenticator application installed on his/her mobile device. It may be better to send a TOPT via SMS; however, this approach may be more expensive.
- Beneficiaries have to be proactive in reporting suspicious behaviour, so they have to be active participants.

- While videos may be sent to children for them to understand the context of their directives, parents or guardians will have to make decisions on their behalf.
- Owing to the ease of access to an e-consent system (as opposed to a traditional paper-based system), a sought-after research subject may become overwhelmed by an inordinate number of requests for access to his/her information.
- The beneficiary is required to be of sound mind and be in a position to make informed choices.

7.4 Summary

This chapter provided an evaluation of the research. The benefits of the research include (i) providing easy access for beneficiaries to control their health information, (ii) providing the means for beneficiaries to report behaviours which violate their human rights; (iii) aiding the medical research process by automating search subject selection, and (iv) tracing activities related to beneficiary information and providing immutable evidence for legal action. The shortcomings of the research were also discussed. The following chapter summarises and concludes the research and, future work is discussed.

Chapter 8

Conclusion

8.1 Introduction

This chapter provides the conclusion of the dissertation and discusses future work. Section 8.2 provides a summary for each of the chapters in the research. Section 8.3 revisits the problem statement and outlines how each of the research questions was addressed. Section 8.4 discusses possible topics for future research. Section 8.5 recaps and outlines the objectives of the research and the contributions are summarised. The dissertation concludes in Section 8.6.

8.2 Dissertation Summary

A summary of each chapter of the dissertation is provided as follows:

- Chapter 1 provided an introduction to the study. A brief overview of the motivation, objectives, the problem statement and research questions were outlined.

- Chapter 2 discussed the overview of the South African healthcare system. The opportunities, challenges and solutions faced by e-health in South Africa were described. The chapter also introduced informed consent and discussed the repercussions for service providers who do not respect the privacy of their patients. Additionally, the chapter provided an overview of consent directive types, attributes and controls.

- Chapter 3 covered information security with a specific focus on principles and legislature that are essential for privacy preservation, such as the PoPIA, Health Professions Act and GDPR. Information security and e-consent go hand in hand as both concepts strive to ensure data privacy. The chapter also provided a discussion of related work. The chapter compares the model and prototype developed for the research against other literature that has conducted similar work.
- Chapter 4 proposed a model for the e-consent management system. The model was designed based on the information gathered from the literature reviews (Chapters 2 and 3). The model presented an abstraction of the proposed system, the function of which is to facilitate customised privacy control for healthcare users making use of electronic healthcare systems. The chapter also illustrated the architectural design for the e-consent management system based on the developed conceptual model.
- Chapter 5 described the implementation of the software prototype developed based on the e-consent conceptual model. The relevant programming languages, application programming interfaces and development environments were described.
- Chapter 6 demonstrated the consent directive life cycle by way of a scenario by detailing its creation, retrieval, update and removal workflows.
- Chapter 7 provided an evaluation of the designed model, architecture and developed software prototype. Furthermore, the benefits and shortcomings of the research were discussed.

- Chapter 8 provides the conclusion of the dissertation and discusses future work.

The next section revisits the problem statement of the research.

8.3 Revisiting the Problem Statement

The problem the dissertation sought to address was the lack of application of informed e-consent in e-health in South Africa. In the age of computing it is becoming more difficult to be in control of the level of privacy of one's information. An approach in healthcare should be available, in a manner similar to the way individuals manage the privacy settings of their social media accounts.

A patient's personal information should only be available to authorised users and the patient should be aware of why the information is being accessed and by whom. Given that South Africa and the rest of the world are moving towards e-health, there is a need for an approach towards privacy preservation through e-consent. This means that a patient should be given an e-consent system to express their consent directives.

The questions that guided this dissertation are listed and addressed below.

- *What is the current state of e-consent in healthcare?*
  The objective of this question was to identify the benefits, challenges and opportunities surrounding e-consent systems in order to determine their value. Chapter 2 motivated the application of e-consent since the continued use of physical documents is not ideal as paper and printing costs are high due to the manual nature of the printing process [127]. Physical documents make patient information difficult to store, search and retrieve [62]. It is also difficult to enforce access control for physical documents as they are more easily accessible for healthcare staff on the premises on the basis that they work there [34]. Furthermore, forms filled in by

hand are often incomplete, inaccurate or illegible. In addition, about 24% of doctors spend less than five minutes informing their patients of procedures and 53% of doctors spend between five and 10 minutes informing their patients even though they should ideally spend at least 30 minutes counselling their patients and allowing enough time for questions and clarifications [24]. Furthermore, a tailor-made consent approach is found to improve the understanding of patients [59]. Therefore, a system like eCMS allows the healthcare beneficiaries to conveniently review their consent directives as some patients agree to a procedure even though they do not understand the full implications of it [59]. Chapter 7 reflected on challenges that may affect the adequate utilisation of eCMS in South Africa, including a lack of familiarity with computer systems, the high cost of bandwidth and a lack of proactive participation by the system users.

- *What challenges do South African healthcare-sector workers experience with regard to e-health?*
  This question aimed to identify the opinions, attitudes and relationship that healthcare workers have with e-health systems. If challenges that broadly affect e-health systems exist, it is unlikely that they will not affect an e-consent system. Chapter 2 identified that challenges to the adoption of e-health systems in South Africa include the absence of ICTs at healthcare facilities, staff lacking ICT-related skills, and old and unreliable computer equipment [104]. While there is hesitation in 72% of physicians that e-health systems may lead to frequent downtime and 64% of them believe that productivity may be hampered, there is a willingness by the staff members to learn how to use e-health systems [104]. The chapter also highlights that if the PU and the PE are absent then the benefits of ICTs cannot be sufficiently realised as its end-users do not value the technology or the end-users simply do not use the system because it is too complex, or there is a lack of user training and knowledge transfer [102].

- *How can privacy-preservation legislature such as the PoPIA be applied in e-consent systems?*
  This question seeks to establish how the relevant privacy legislature should be integrated into the developmental life cycle so that the e-consent solution is developed inline with privacy laws. Chapter 3 selected the Health Professions Act and PoPIA as the main Acts to influence this research. The PoPIA is based on the best features of international privacy legislatures and OECD guidelines for the protection of privacy. The PoPIA principles are also aligned with the GDPR. The PoPIA comprises eight information-processing principles, which were included in the model, architectural design and prototype presented in Chapters 4 to 6. The PoPIA principles were implemented using the information security services and mechanisms described in Chapter 3.

- *In what way can interoperable e-consent systems be implemented in South Africa?*
  This question seeks to identify implementation guidelines that will facilitate interoperability in an e-consent management system. South African e-health systems suffer from a lack of uniformity [104]. The lack of the use of standards means that different software applications cannot communicate and exchange information with each other with ease. Chapter 3 explains that HL7 International is an accredited body that sets up standards for the transfer of clinical and administrative data between healthcare software applications. Thus, HL7 was used in the eCMS.

Therefore, given that the research questions have been resolved, the entire problem statement has been fully addressed.

8.4 Future Work

Given that the focus of this research was the privacy preservation of beneficiaries, there is an opportunity to explore implementation for medical treatment and advanced care directives, which are the different types of consent directives not focused on in this research. Directives for medical treatment involve obtaining electronic consent from beneficiaries for healthcare procedures such as surgery or radiation therapy. Generally, the procedures mentioned previously are medium to high risk and giving written consent through a system such as eCMS (i) makes the health practitioners accountable and (ii) provides the patient and health provider with a record of that to which the patient consented. If the patient was informed that his/her left leg would be amputated, and the right leg was amputated, this would be grounds to accuse the hospital of doing grievous bodily harm.

Another opportunity for growth for eCMS is for the system to account for advanced care medical directives. If the patient has an order for "do not resuscitate" or "do not intubate" or other end-of-life directives, those should be respected and can easily be retrieved electronically. Future e-consent management systems may consider centralisation of requests in order to reduce the number of identical requests submitted to an individual.

8.5 Research Contributions

The specific objectives that were pursued as part of the main objective are as follows:

- Analyse existing work on e-consent, interoperability, information security and privacy-preserving legislature and principles.
- Conduct a research survey that will give information on the current state of e-consent in South Africa.
- Design an e-consent management system model.
- Develop a prototype of the e-consent management system model as proof of concept.

Ultimately, a secure, user-friendly, informative, controllable, modifiable and privacy preserving consent management system was developed.

Health information systems enable the collection and use of electronic health data, which, in turn, provides benefits to various stakeholders [42, 51, 66]. In most cases, the electronic health data found in medical systems is patient data. With the patients' data being exchanged electronically, the patients still need a way to consent who should and who should not access their data. This requires an electronic consent management mechanism, and with a proper consent management in place, the following will result:

- Medical researchers can conduct their work more efficiently as there is increased access to accurate information. Additionally, researchers can use available data to investigate how high-quality and cost-effective healthcare may be provided.
- The quality of clinical care is improved as immediate access to information enables quick and informed decision-making regarding diagnoses and treatments for healthcare service providers.
- Patients can benefit by making informed decisions about service providers, medical treatments and health conditions in general.

8.6 Final Remarks

The objective of this dissertation was to design and develop an e-Consent Management System that facilitates customised privacy control for healthcare users making use of electronic healthcare systems. The developed eCMS is an efficient and practical application for informed e-consent in e-health in South Africa.

This chapter concludes the study. The subsequent sections provide the bibliography and the list of acronyms used in the literature.

Bibliography

[1] Raja Manzar Abbas, Noel Carroll, Ita Richardson, and Sarah Beecham. The need for trustworthiness models in healthcare software solutions. In *HEALTHINF*, pages 451–456, 2017.

[2] Mehmet Adalier and Scott Burleigh. Cross-domain autonomous communication protocol for delay tolerant networks. In *NAECON 2018-IEEE National Aerospace and Electronics Conference*, pages 124–131. IEEE, 2018.

[3] Trina Adams, Martin Budden, Chris Hoare, and Hugh Sanderson. Lessons from the central hampshire electronic health record pilot project: issues of data protection and consent. *Bmj*, 328(7444):871–874, 2004.

[4] Statistics South Africa. General household survey. https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Accessed: 2019-05-21.

[5] Jenny C Aker, Ishita Ghosh, and Jenna Burrell. The promise (and pitfalls) of ict for agriculture initiatives. *Agricultural Economics*, 47(S1):35–48, 2016.

[6] Warrick Asher. How does the gdpr affect south africa? http://www.barnowl.co.za/insights/how-does-the-gdpr-affect-south-africa/. Accessed: 2018-11-21.

[7] Hanieh Azkia, Nora Cuppens-Boulahia, Frédéric Cuppens, and Gouenou Coatrieux. Reconciling ihe-atna profile with a posteriori contextual access and usage control policy in healthcare environment. In *2010 Sixth International Conference on Information Assurance and Security*, pages 197–203. IEEE, 2010.

[8] Hanieh Azkia, Nora Cuppens-Boulahia, Frédéric Cuppens, Gouenou Coatrieux, and Said Oulmakhzoune. Deployment of a posteriori access control using ihe atna. *International Journal of Information Security*, 14(5):471–483, 2015.

[9] Carolyn Baek, Vuyiswa Mathambo, Sibongile Mkhize, Irwin Friedman, Louis Apicella, and Naomi Rutenberg. Key findings from an evaluation of the mothers2mothers program in kwazulu-natal, south africa. 2007.

[10] Soma Bandyopadhyay and SS Thakur. Ict in education: Open source software and its impact on teachers and students. *International Journal of Computer Applications*, 151(6), 2016.

[11] Matt Behrens. Understanding the 3 main types of encryption. https://spin.atomicobject.com/2014/11/20/encryption-symmetric-asymmetric-hashing/. Accessed: 2018-12-13.

[12] Aissam Belghiat and Allaoua Chaoui. A graph transformation of activity diagrams into π-calculus for verification purpose. In *ICAASE*, pages 107–114, 2018.

[13] Joachim Bergmann, Oliver J Bott, Dietrich P Pretschner, and Reinhold Haux. An e-consent-based shared ehr system architecture for integrated healthcare networks. *International journal of medical informatics*, 76(2):130–136, 2007.

[14] Valentin Bojinov. *RESTful Web API Design with Node. js.* Packt Publishing Ltd, 2016.

[15] Natalie T Boutin, Kathleen Mathieu, Alison G Hoffnagle, Nicole L Allen, Victor M Castro, Megan Morash, P Pearl O'Rourke, Elizabeth L Hohmann, Neil Herring, Lynn Bry, et al. Implementation of electronic consent at a biobank: an opportunity for precision medicine research. *Journal of personalized medicine*, 6(2):17, 2016.

[16] Laura Bresser, Steffen Köhler, and Christoph Schwaab. The development of an application for data privacy by applying an audit repository based on ihe atna. In *eHealth*, pages 219–225, 2014.

[17] Okan Bursa, Emine Sezer, Ozgu Can, and Murat Osman Unalir. Using foaf for interoperable and privacy protected healthcare information systems. In *Research Conference on Metadata and Semantics Research*, pages 154–161. Springer, 2014.

[18] M Buys. Protecting personal information: Implications of the protection of personal information (popi) act for healthcare professionals. *SAMJ: South African Medical Journal*, 107(11):954–956, 2017.

[19] Ozgu Can. A semantic model for personal consent management. In *Metadata and Semantics Research: 7th International Conference, MSTR 2013, Thessaloniki, Greece, November 19-22, 2013. Proceedings*, volume 390, page 146. Springer, 2013.

[20] Nicole B Carbone, Joseph Njala, Debra J Jackson, Michael T Eliya, Chileshe Chilangwa, Jennifer Tseka, Tasila Zulu, Jacqueline R Chinkonde, Judith Sherman, Chifundo Zimba, et al. "i would love if there was a young woman to encourage us, to ease our anxiety which we would have if we were alone": Adapting the mothers2mothers mentor mother model for adolescent mothers living with hiv in malawi. *PloS one*, 14(6), 2019.

[21] Samuel Carter. Rbac vs abac access control models - iam explained. http://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained. Accessed: 2018-12-13.

[22] Ann Cavoukian. Privacy by design. *Take the challenge. Information and privacy commissioner of Ontario, Canada*, 2009.

[23] SC Chima et al. " because i want to be informed, to be part of the decision-making": Patients' insights on informed consent practices by healthcare professionals in south africa. *Nigerian journal of clinical practice*, 18(7):46, 2015.

[24] Sylvester C Chima. Evaluating the quality of informed consent and contemporary clinical practices by medical doctors in south africa: An empirical study. *BMC medical ethics*, 14(S1):S3, 2013.

[25] Enrico Coiera and Roger Clarke. e-consent: The design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association*, 11(2):129–140, 2004.

[26] Secure Software Concepts. Discretionary access control vs mandatory access controls. https://sites.google.com/site/jimmyxu101/concepts/accesscontrol/. Accessed: 2018-12-13.

[27] cryptomathic. What is non-repudiation? https://www.cryptomathic.com/products/authentication-signing-digital-signatures-faqs/what-is-non-repudiation. Accessed: 2018-11-13.

[28] CSO. The 17 biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, 2018. Accessed: 2018-06-08.

[29] Dylan Curran. Are you ready? here is all the data facebook and google have on you. https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy, 2018. Accessed: 2018-06-08.

[30] Georg Disterer. Iso/iec 27000, 27001 and 27002 for information security management. 2013.

[31] docusign. Understanding digital signatures. https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq. Accessed: 2019-02-18.

[32] N El Ioini, C Pahl, and Sven Helmer. A decision framework for blockchain platforms for iot and edge computing. SCITEPRESS, 2018.

[33] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. Preserving the privacy of patient records in health monitoring systems. In *Theory and Practice of Cryptography Solutions for Secure Information Systems*, pages 499–529. IGI Global, 2013.

[34] Sigurd Eskeland and Vladimir A Oleshchuk. Epr access authorization of medical teams based on patient consent. In *ECEH*, pages 11–22, 2007.

[35] Jorge Muriel Fernandez, María José Sánchez Ledesma, Manuel López Millan, and María Begoña García Cenador. Study of the uses of information and communication technologies by pain treatment unit physicians. *Journal of medical systems*, 41(5):78, 2017.

[36] José Luis Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, and Ambrosio Toval. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3):541–562, 2013.

[37] FindLaw. Is there a difference between confidentiality and privacy? https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html. Accessed: 2018-11-13.

[38] Albana Gaba, Yeb Havinga, Henk-Jan Meijer, and Evert Jan. Privacy and security for analytics on healthcare data. 2014.

[39] Yaorong Ge, David K Ahn, Bhagyashree Unde, H Donald Gage, and J Jeffrey Carr. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *Journal of the American Medical Informatics Association*, 20(1):157–163, 2013.

[40] Arash Ghazvini and Zarina Shukur. Security challenges and success factors of electronic healthcare system. *Procedia Technology*, 11:212–219, 2013.

[41] Stefan Gossling. Ict and transport behaviour: A conceptual review. *International Journal of Sustainable Transportation*, (just-accepted):00–00, 2017.

[42] Lawrence O Gostin. National health information privacy: regulations under the health insurance portability and accountability act. *JAMA*, 285(23):3015–3021, 2001.

[43] Jeevarathnam P Govender. The adoption of internet banking in a developing economy. *Journal of economics and behavioral studies*, 5(8):496–504, 2013.

[44] Western Cape Goverment. New project connects expectant moms to government health services. https://www.westerncape.gov.za/general-publication/new-project-connects-expectant-moms-to-government-health-service, 2014. Accessed: 2018-09-27.

[45] Nelson Hastings, Rene Peralta, Stefan Popoveniuc, and Andrew Regenscheid. Security considerations for remote electronic uocava voting. *National Institute of Standards and Technology (NIST), US Department of Commerce., NISTIR*, 7770, 2011.

[46] ACT Health. Informed consent. http://www.health.act.gov.au/public-information/consumers/informed-consent. Accessed: 2018-03-22.

[47] health.vic. Standard 1 governance for safety and quality in health service organisations. https://www2.health.vic.gov.au/about/publications/policiesandguidelines/Standard%201%20Governance%20for%20Safety%20and%20Quality%20in%20Health%20Service%20Organisations, 2015. Accessed: 2018-09-27.

[48] O Heinze and B Bergh. A model for consent-based privilege management in personal electronic health records. *Studies in health technology and informatics*, 205:413–417, 2014.

[49] Oliver Heinze, Markus Birkle, Lennart Köster, and Björn Bergh. Architecture of a consent management suite and integration into ihe-based regional health information networks. *BMC medical informatics and decision making*, 11(1):58, 2011.

[50] HL7. Fhir release 3 (stu). http://www.hl7.org/fhir/consent.html. Accessed: 2018-09-27.

[51] James G Hodge Jr, Lawrence O Gostin, and Peter D Jacobson. Legal issues concerning electronic health information: privacy, quality, and liability. *Jama*, 282(15):1466–1471, 1999.

[52] HPCSA. About hpcsa. http://www.hpcsa.co.za/About. Accessed: 2018-11-14.

[53] Lianne Lian Hu, Steven Sparenborg, and Betty Tai. Privacy protection for patients with substance use problems. *Substance abuse and rehabilitation*, 2:227, 2011.

[54] Chinwe Juliana Iwu, Ntombenhle Ngcobo, Sara Cooper, Lindi Mathebula, Hlokoma Mangqalaza, Abongile Magwaca, Usuf Chikte, and Charles S Wiysonge. Mobile reporting of vaccine stock-levels in primary health care facilities in the

eastern cape province of south africa: perceptions and experiences of health care workers. *Human Vaccines & Immunotherapeutics*, pages 1–7, 2020.

[55] M Jobson. Structure of the health system in south africa. *Johannesburg: Khulumani support group*, 2015.

[56] Simon Josefsson et al. The base16, base32, and base64 data encodings. Technical report, RFC 4648, October, 2006.

[57] Yi-Yun Ko and Der-Ming Liou. The study of managing the personal consent in the electronic healthcare environment. *World Academy of Science, Engineering and Technology*, 65:314, 2010.

[58] Heng Wei Lee, Thurasamy Ramayah, and Nasriah Zakaria. External factors in hospital information system (his) adoption model: a case on malaysia. *Journal of medical systems*, 36(4):2129–2140, 2012.

[59] Yen-Ko Lin, Chao-Wen Chen, Wei-Che Lee, Yuan-Chia Cheng, Tsung-Ying Lin, Chia-Ju Lin, Leiyu Shi, Yin-Chun Tien, and Liang-Chi Kuo. Educational video-assisted versus conventional informed consent for trauma-related debridement surgery: a parallel group randomized controlled trial. *BMC medical ethics*, 19(1):23, 2018.

[60] Auqib Hamid Lone and Roohie Naaz Mir. Forensic-chain: ethereum blockchain based digital forensics chain of custody. *Sci. Pract. Cyber Secur. J*, 2018.

[61] Isabel Maria Lopes, T Guarda, and P Oliveira. Implementation of iso 27001 standards as gdpr compliance facilitator. *Journal of Information Systems Engineering & Management*, 2(4):1–8, 2019.

[62] Kapil Chalil Madathil, Reshmi Koikkara, Jihad Obeid, Joel S Greenstein, Iain C Sanderson, Katrina Fryar, Jay Moskowitz, and Anand K Gramopadhye. An inves-

tigation of the efficacy of electronic consenting interfaces of research permissions management system in a hospital setting. *International journal of medical informatics*, 82(9):854–863, 2013.

[63] EA Mantzaris. A matter of life and death-pharmaceutical supply chain and procurement corruption in south africa. *African Journal of Public Affairs*, 11(2):63–82, 2019.

[64] A Haeri Mazanderani, GG Sherman, F Moyo, Ameena Ebrahim Goga, and U Feucht. Leveraging the road to health booklet as a unique patient identifier to monitor the prevention of mother-to-child transmission programme. *South African Medical Journal*, 108(9), 2018.

[65] Nathan McDonald. Digital in 2018: World's internet users pass the 4 billion mark. https://wearesocial.com/us/blog/2018/01/global-digital-report-2018, 2018. Accessed: 2018-06-08.

[66] Deven McGraw. Privacy and health information technology: Executive summary. *The Journal of Law, Medicine & Ethics*, 37(2_suppl):121–149, 2009.

[67] Er Mense, Bernd Blobel, et al. Hl7 standards and components to support implementation of the european general data protection regulation (gdpr). *European Journal of Biomedical Informatics*, 13(1), 2017.

[68] Adigun Miss, Adeyinka Olubunmi, and Temitope Samnuel. The impact of ict usage in improving advertising strategies in selected media house: A case study of splash fm (105.5). 2017.

[69] I Moodley. An hiv-free generation: review of prevention strategies. *South African Family Practice*, pages 15–20, 2019.

[70] Laura Moss, Martin Shaw, Ian Piper, Christopher Hawthorne, and John Kinsella. Sharing of big data in healthcare: Public opinion, trust, and privacy considerations for health informatics researchers. In *HEALTHINF*, pages 463–468, 2017.

[71] Martin K Mwila and Perseverance Mbewe. Design and implementation of a node. js based communication framework for an unmanned autonomous ground vehicle. In *2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech)*, pages 74–79. IEEE, 2017.

[72] Ayaz Nanji. The incredible amount of data generated online every minute [infographic]. https://www.marketingprofs.com/charts/2017/32531/the-incredible-amount-of-data-generated-online-every-minute-infographic, 2017. Accessed: 2018-06-08.

[73] Rita Noumeir. Integrating the healthcare enterprise process. *International Journal of Healthcare Technology and Management*, 9(2):167–180, 2008.

[74] Yvonne O'Connor, Wendy Rowan, Laura Lynch, and Ciara Heavin. Privacy by design: Informed consent and internet of things for smart health. *Procedia Computer Science*, 113:653–658, 2017.

[75] OECD. Oced privacy guidelines. https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Accessed: 2019-05-06.

[76] Press Office: UCT Graduate School of Business. South africa's healthcare system could be world class. http://www.gsb.uct.ac.za/rolene-wagner-dsp. Accessed: 2018-05-23.

[77] Government of South Africa. Health. https://www.gov.za/issues/health. Accessed: 2020-03-03.

[78] Christine OKeefe, Andrew Goodchild, Paul Greenfield, Andrew Waugh, Eddy Cheung, and Donaugh Austin. Implementation of electronic consent mechanisms. *Final Analysis Paper*, 2002.

[79] Christine M O'Keefe, Paul Greenfield, and Andrew Goodchild. A decentralised approach to electronic consent and health information access control. *Journal of Research and Practice in Information Technology*, 37(2):161, 2005.

[80] Don O'Mahony, Graham Wright, Parimalarani Yogeswaran, and Frederick Govere. Knowledge and attitudes of nurses in community health centres about electronic medical records. *curationis*, 37(1):01–06, 2014.

[81] opentext. Information security and privacy. https://www.opentext.com/products-and-solutions/business-needs/information-governance/ensure-compliance/information-security-and-privacy. Accessed: 2018-11-13.

[82] Toks Oyedemi. Participation, citizenship and internet use among south african youth. *Telematics and Informatics*, 32(1):11–22, 2015.

[83] Danny Palmer. What is gdpr? everything you need to know about the new general data protection regulations. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/. Accessed: 2018-11-21.

[84] Eun Hee Park, Jongwoo Kim, and Young Soon Park. The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, 65:64–76, 2017.

[85] Pheobe Parke. More africans have access to cell phone service than piped water. https://edition.cnn.com/2016/01/19/africa/africa-afrobarometer-infrastructure-report/index.html, 2016. Accessed: 2018-06-08.

[86] Charles P Pfleeger and Shari Lawrence Pfleeger. *Analyzing computer security: a threat/vulnerability/countermeasure approach*. Prentice Hall Professional, 2012.

[87] Yogan Pillay, Joanne Peter, and Peter Barron. Using mobile technology to improve maternal, child and youth health and treatment of hiv patients: guest editorial. *African Journal of Health Professions Education*, 106(1):3–4, 2016.

[88] PostgreSQL. Postgresql: The world's most advanced open source relational database. https://www.postgresql.org/. Accessed: 2019-10-01.

[89] Cédric Pruski. e-crl: A rule-based language for expressing patient electronic consent. In *eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10. Second International Conference on*, pages 141–146. IEEE, 2010.

[90] Aarthu Ramdhin. Protection of personal information bill: what should you be asking? https://www.werksmans.com/legal-briefs-view/protection-of-personal-information-bill-what-should-you-be-asking/. Accessed: 2018-03-01.

[91] Shandir Ramlagan, Violeta J Rodriguez, Karl Peltzer, Robert AC Ruiter, Deborah L Jones, and Sibusiso Sifunda. Self-reported long-term antiretroviral adherence: A longitudinal study among hiv infected pregnant women in mpumalanga, south africa. *AIDS and Behavior*, 23(9):2576–2587, 2019.

[92] Enos M Rampamba, Johanna C Meyer, Brian Godman, Amanj Kurdi, and Elvera Helberg. Evaluation of antihypertensive adherence and its determinants at primary healthcare facilities in rural south africa. *Journal of comparative effectiveness research*, 7(7):661–672, 2018.

[93] James Redwood, Sasha Thelning, Abbas Elmualim, and Stephen Pullen. The proliferation of ict and digital technology systems and their influence on the dynamic capabilities of construction firms. *Procedia Engineering*, 180:804–811, 2017.

[94] Thomas C Rindfleisch. Privacy, information technology, and health care. *Communications of the ACM*, 40(8):92–100, 1997.

[95] Fiona Riordan, Chrysanthi Papoutsi, Julie E Reed, Cicely Marston, Derek Bell, and Azeem Majeed. Patient and public attitudes towards informed consent models and levels of awareness of electronic health records in the uk. *International journal of medical informatics*, 84(4):237–247, 2015.

[96] Jitesh Rohatgi. Gdpr and healthcare: Understanding health data and consent. https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent. Accessed: 2018-11-21.

[97] Margaret Rose. access control. https://searchsecurity.techtarget.com/definition/access-control. Accessed: 2018-10-11.

[98] Margaret Rouse. homomorphic encryption. https://searchsecurity.techtarget.com /definition/homomorphic-encryption. Accessed: 2018-12-13.

[99] Chun Ruan and Sang-Soo Yeo. Modeling of an intelligent e-consent system in a healthcare domain. *J. UCS*, 15(12):2429–2444, 2009.

[100] Giovanni Russello, Changyu Dong, and Naranker Dulay. Consent-based workflows for healthcare management. In *Policies for Distributed Systems and Networks, 2008. POLICY 2008. IEEE Workshop on*, pages 153–161. IEEE, 2008.

[101] Nkqubela Ruxwana, Marlien Herselman, and Dalenca Pottas. Generic quality assurance model (gqam) for successful e-health acquisition in rural hospitals. IADIS International Conference on eHealth, 2011.

[102] Nkqubela L Ruxwana, Marlien E Herselman, and D Pieter Conradie. Ict applications as e-health solutions in rural healthcare in the eastern cape province of south africa. *Health information management journal*, 39(1):17–29, 2010.

[103] Surbhi S. Difference between privacy and confidentiality. https://keydifferences.com/difference-between-privacy-and-confidentiality.html. Accessed: 2018-11-20.

[104] Michael Sello Seahloli. *Current Status of Medical Informatics and Implementing Electronic Healthcare Records, Challenges and Future Direction in South Africa*. PhD thesis, 2017.

[105] Christopher Seebregts, Pierre Dane, Annie Neo Parsons, Thomas Fogwill, Debbie Rogers, Marcha Bekker, Vincent Shaw, and Peter Barron. Designing for scale: optimising the health information system architecture for mobile maternal health messaging in south africa (momconnect). *BMJ global health*, 3(Suppl 2):e000563, 2018.

[106] Robert H Shelton. Electronic consent channels: preserving patient privacy without handcuffing researchers. *Science translational medicine*, 3(69):69cm4–69cm4, 2011.

[107] Elme Smith and Jan HP Eloff. Security in health-care information systems—current trends. *International journal of medical informatics*, 54(1):39–54, 1999.

[108] ER St John, AJ Scott, TE Irvine, F Pakzad, DR Leff, and GT Layer. Completion of hand-written surgical consent forms is frequently suboptimal and could be improved by using electronically generated, procedure-specific forms. *the surgeon*, 15(4):190–195, 2017.

[109] Belinda Strydom, Fanie Hendriksz, and Shabir Banoo. Innovation to solution: the radu journey. *SA Pharmaceutical Journal*, 85(3):43–44, 2018.

[110] Felix Sukums, Nathan Mensah, Rose Mpembeni, Siriel Massawe, Els Duysburgh, Afua Williams, Jens Kaltschmidt, Svetla Loukanova, Walter E Haefeli, and Antje Blank. Promising adoption of an electronic clinical decision support system

for antenatal and intrapartum care in rural primary healthcare facilities in subsaharan africa: The qualmat experience. *International journal of medical informatics*, 84(9):647–657, 2015.

[111] technopedia. Hashing. https://www.techopedia.com/definition/14316/hashing. Accessed: 2018-11-21.

[112] technopedia. Information privacy. https://www.techopedia.com/definition/10380 /information-privacy. Accessed: 2018-11-13.

[113] technopedia. Strong authentication. https://www.techopedia.com/ definition/23939/strong-authentication. Accessed: 2019-02-15.

[114] Techotopia. Mandatory, discretionary, role and rule based access control. https://www.techotopia.com/index.php/Mandatory, _Discretionary,_Role_and_Rule_Based_Access_Control. Accessed: 2018-10-11.

[115] Right to care. Medication atms launched in sa: patient waiting times cut to under 3 minutes. https://www.righttocare.org/press-releases/medication-atms-launched-in-sa-patient-waiting-times-cut-to-under-3-minutes, 2018. Accessed: 2018-09-25.

[116] Mogamat Yoesrie Toefy. Development and testing of an m-health platform to reduce post-operative penetrative sex in recipients of voluntary medical male circumcision. 2017.

[117] BA Townsend and RE Scott. The development of ethical guidelines for telemedicine in south africa. *South African Journal of Bioethics and Law*, 12(1):19–26, 2019.

[118] Alison Treadaway. Getting gdpr-ready was painful, but popi compliance is yet to follow. https://memeburn.com/2018/06/gdpr-south-africa-popi-businesses/. Accessed: 2018-12-13.

[119] Christopher Tredger. Africa's limited data protection laws heighten gdpr significance. https://www.itweb.co.za/content/LPwQ5MlyAxbqNgkj. Accessed: 2020-02-29.

[120] Nicole Van Deursen, William J Buchanan, and Alistair Duff. Monitoring information security risks within health care. *computers & security*, 37:31–45, 2013.

[121] Christel van Wyk. Where to with the nhi and medical credits? *Tax Breaks Newsletter*, 2018(387):1–2, 2018.

[122] VCloudNews. Every day big data statistics - 2.5 quintilion bytes of data created daily. http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/, 2015. Accessed: 2018-06-08.

[123] Dan S Wamala and Kaddu Augustine. A meta-analysis of telemedicine success in africa. *Journal of pathology informatics*, 4, 2013.

[124] LW Wang. The privacy rule: Hipaa standards for the privacy of individually identifiable health information. *Employee benefits journal*, 27(3):59–63, 2002.

[125] Graham Wright, Don O'Mahony, and Liezel Cilliers. Electronic health information systems for public health care in south africa: a review of current operational systems. *Journal of Health Informatics in Africa*, 4(1), 2017.

[126] Bo Yu, Duminda Wijesekera, and Paulo Costa. Consent-based workflow control in emrs. *Procedia Technology*, 16:1434–1445, 2014.

[127] Bo Yu, Duminda Wijesekera, and Paulo Cesar G Costa. Informed consent in electronic medical record systems. In *Healthcare Ethics and Training: Concepts, Methodologies, Tools, and Applications*, pages 1029–1049. IGI Global, 2017.

[128] Bo Yu, Duminda Wijesekera, and Paulo CG Costa. An ontology for medical treatment consent. In *STIDS*, pages 72–79, 2014.

[129] Buket Yüksel, Alptekin Küpçü, and Öznur Özkasap. Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68:1–13, 2017.

[130] Shams Zawoad and Ragib Hasan. Digital forensics in the age of big data: Challenges, approaches, and opportunities. In *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*, pages 1320–1325. IEEE, 2015.

[131] Gang Zhou, Harald Michalik, and Laszlo Hinsenkamp. Efficient and high-throughput implementations of aes-gcm on fpgas. In *2007 International Conference on Field-Programmable Technology*, pages 185–192. IEEE, 2007.

[132] Manoush Zomorodi. Do you know how much private information you give away every day? http://time.com/4673602/terms-service-privacy-security/, 2017. Accessed: 2018-06-08.

Appendix A

Acronyms

AES-GCM Advanced Encryption Standard with Galois/Counter Mode.

ANN Artificial Neural Network.

ARV Antiretroviral.

ATNA Audit Trail and Node Authentication.

CRC Cyclic Redundancy Check.

e-CRL e-Consent Rule-Based Language.

eCMS e-Consent Management System.

EHR Electronic Health Record.

GDPR General Data Protection Regulation.

GPS Global Positioning System.

HIS Health Information System.

HIV Human Immunodeficiency Virus.

HL7 Health Level-7.

HPCSA Health Professions Council of South Africa.

HPRS Health Patient Registration System.

HR Human Resources.

ICTs Information and Communication Technologies.

ID Identity Document.

IHE Integrated Health Exchange.

IoT Internet of Things.

IT Information Technology.

m2m Mothers2Mothers.

MD5 Message Digest 5.

MPI Master Patient Index.

NHI National Health Insurance.

OECD Organisation for Economic Cooperation and Development.

PbD Privacy by Design.

PDU Pharmacy Dispensing Unit.

PE Perceived ease of use.

PIN Personal Identification Number.

PoPIA Protection of Personal Information Act.

PU Perceived usefulness.

SHA Secure Hashing Algorithm.

SMS Short Messaging Service.

SVS Stock Visibility System.

TB Tuberculosis.

Appendix B

Derived Publications

The following list includes a list of the publications derived from this dissertation.

- Lelethu Zazaza, H.S Venter and George Sibiya. The current state of electronic consent systems in e-Health for privacy preservation. In *International Information Security Conference*, pages 76–88. Springer, 2018.
- Lelethu Zazaza, H.S Venter, and George Sibiya. A Conceptual Model for Consent Management in South African e-Health Systems for Privacy Preservation. *In International Information Security Conference*, pages 69–82. Springer, 2019.