Designing and Implementing an Information Accountability Framework for Usable and Useful eHealth Systems

Daniel K. Grunwell
BIT

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Electrical Engineering and Computer Science
Faculty of Science and Engineering
Queensland University of Technology
2017

Keywords

Access control, eHealth, electronic health records, information accountability, information privacy, information security, usability, usable security

Abstract

The sharing of health information and the wide adoption of eHealth systems has the potential to improve healthcare by ensuring a high availability of information and lowering costs. However, at present, there are competing information access requirements between healthcare consumers (i.e. patients) and healthcare professionals. While consumers want control over who can access their information and how it is used, healthcare professionals desire prompt access to as much information as required in order to make well-informed decisions and provide quality care.

In order to balance these requirements, an Information Accountability Framework (IAF) devised for eHealth systems has been proposed. Through the use of Information Accountability protocols, so-called Accountable-eHealth systems (AeH) aim to create an eHealth environment where health information is available to the right person at the right time without rigid barriers whilst empowering the consumers with information control and transparency.

I explored the design and implementation of usable and useful AeH systems through the implementation of a prototype of the IAF. An investigation applying a standard usability study method with the 'think aloud' protocol and a semi-structured interview was completed using this prototype with 20 participants filling the patient role. From this, usability issues were identified in the prototype, though the system was found to be quite usable by patients overall. The majority of participants believed that the accountability aspects sufficiently protected their privacy, while ensuring healthcare professionals had the information they needed.

I further investigated the implementation of the IAF protocols and demonstrated their functionality in two different existing eHealth systems. This demonstrates that it is possible to modify existing eHealth systems to incorporate the IAF protocols. It was also found that the evaluated eHealth systems did not have existing accountability mechanisms that provided non-repudiation and proactive auditing for misuse. Using one of the implementations, a pilot study with five healthcare professionals was performed. The participating doctors were positive about the potential of the IAF protocols and provided valuable insight into the possibilities and challenges of implementing such a system.

Accountable-eHealth systems enable the creation of eHealth records that can be useful to both patients and healthcare professionals by balancing their information access requirements. This research advances the knowledge of the implementation of AeH systems with the aim of enabling the creation of more useful eHealth systems.

Contents

List of Figures

List of Listings

List of Tables

List of Abbreviations

- ACL – Access Control List
- AeH – Accountable eHealth
- AMA – Australian Medical Association
- DAC – Discretionary Access Control
- DBMS – Database Management System
- DFD – Data flow diagram
- DHT – Distributed Hash Table
- DoS – Denial-of-service
- DRM – Digital Rights Management
- EHR – Electronic Health Record
- EMR – Electronic Medical Record
- EPAL – Enterprise Privacy Authorization Language
- HA – Health Authority (i.e. government health department)
- HBDA – Health Big Data Analytics
- HCP – Healthcare Professional
- HITECH – Health Information Technology for Economic and Clinical Health Act
- HMAC – Hash-based message authentication code
- IA – Information Accountability
- IAF – Information Accountability Framework
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System
- MAC – Mandatory Access Control

- ODRL – Open Digital Rights Language
- PBAC – Purpose-Based Access Control
- PCEHR – Personally Controlled Electronic Health Record
- PKC – Public Key Cryptography
- RBAC – Role-Based Access Control
- SEHR – Shared Electronic Health Record
- SoD – Separation of duties
- ToT – Time on Task
- WHO – World Health Organisation
- XACML – eXtensible Access Control Markup Language
- XML – eXtensible Markup Language

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

QUT Verified Signature

Signature:

Date: 2016-12-20

Acknowledgements

I would like to thank my supervisors Dr. Tony Sahama and Dr. Leonie Simpson for their invaluable advice and support throughout my PhD. Thank you to Randike Gajanayake who provided a rich base on which to begin my research and provided me with invaluable advice and feedback at the beginning of my journey. I would also like to thank our research partners in Brazil, Sergio Campos and Paulo Batista, for their amazing work and support during our collaboration. Additional thanks to Andre Kushniruk, Mu-Hsing Kuo, and Elizabeth Borycki for their collaboration early in my PhD, and particularly to Andre for his advice on usability studies.

I would like to thank my partner, Samantha, for her unending love and support, and for listening patiently and providing encouragement during my struggles. I would like to thank my parents and family for being a constant source of support and encouragement.

Finally, I would like to thank all the reviewers, panel members within QUT, and other researchers who have provided valuable feedback on my work.

Publications Arising from this Thesis

The outcomes of this thesis have been published or are under review in peer-reviewed journals and conferences.

Published Papers

Refereed Journal Papers

1. Kuo, Mu-Hsing, Sahama, Tony, Kushniruk, Andre, Borycki, Elizabeth, and **Grunwell, Daniel** (2014) Health Big Data Analytics: Current Perspectives, Challenges and Potential Solutions. *International Journal of Big Data Intelligence (IJBDI)*, 1(1/2):114–126.

Refereed Conference Papers

2. **Grunwell, Daniel**, and Sahama, Tony (2016) Delegation of access in an Information Accountability Framework for eHealth. In *Proceedings of the Ninth Australasian Workshop on Health Informatics and Knowledge Management (HIKM 2016)*, Australian Computer Society, Australia.

3. **Grunwell, Daniel**, Batista, Paulo, Campos, Sergio, and Sahama, Tony (2015) Managing and Sharing Health Data through Information Accountability Protocols. In *Proceedings of the 17th International Conference on E-health Networking, Application and Services (Healthcom)*, IEEE, Boston, USA.

4. **Grunwell, Daniel**, and Sahama, Tony (2015) Information Accountability and Health Big Data Analytics: A Consent-Based Model. In *Proceedings of the 17th International Conference on E-health Networking, Application and Services (Healthcom)*, IEEE, Boston, USA.

5. **Grunwell, Daniel**, Gajanayake, Randike, and Sahama, Tony (2015) The security and privacy of usage policies and provenance logs in an Information Ac-

countability Framework. In *Proceedings of the Eighth Australasian Workshop on Health Informatics and Knowledge Management (HIKM 2015)*, Australian Computer Society, Sydney, Australia.

6. **Grunwell, Daniel**, Gajanayake, Randike, and Sahama, Tony (2014) Demonstrating Accountable-eHealth Systems. In *Proceedings of the 2014 IEEE International Conference on Communications (ICC)*, IEEE, Sydney, Australia.

Refereed Conference Tutorials

7. **Grunwell, Daniel** & Sahama, Tony R. (2015) The design and implementation of an Information Accountability Framework for eHealth systems. In IEEE Healthcom 2015 17th International Conference on E-Health Networking, Application & Services, 15-18 October 2014, Natal, Brazil.

8. **Grunwell, Daniel** & Sahama, Tony R. (2014) Designing and implementing usable and useful Accountable-eHealth systems. In IEEE Healthcom 2014 16th International Conference on E-Health Networking, Application & Services, 15-18 October 2014, Natal, Brazil.

9. Gajanayake, Randike, Sahama, Tony R., Lane, Bill, and **Grunwell, Daniel** (2013) Designing an information accountability framework for eHealth. At the *IEEE Healthcom 2013 15th International Conference on E-Health Networking, Application & Services*, 9-12 October 2013, Instituto Superior de Ciências Sociais e Políticas – Technical University of Lisbon, Lisbon, Portugal.

Refereed Conference Posters

10. Batista, Paulo, **Grunwell, Daniel**, Sahama, Tony, and Campos, Sergio (2015) Medical Data Access Accountability in EHR Systems, A Practical Perspective.

In *X-Meeting 2015 - 11th International Conference of the AB3C + Brazilian Symposium of Bioinformatics*, 3-6 November 2015, Sao Paulo, Brazil.

11. **Grunwell, Daniel**, Gajanayake, Randike, and Sahama, Tony (2015) The security and privacy of usage policies and provenance logs in an Information Accountability Framework. In *Australian Computer Science Week (ACSW) Doctoral Consortium*, Australian Computer Society, Sydney, Australia.

12. **Grunwell, Daniel**, Gajanayake, Randike, and Sahama, Tony (2013) Achieving Meaningful Use of eHealth through Accountable-eHealth (AeH) Systems. Presented at the Health Roundtable 2013 Innovation Workshops and Awards, November 8 2013.

13. Sahama, Tony, **Grunwell, Daniel**, and Gajanayake, Randike (2013) An Information Accountability perspective to eHealth Security and Privacy. Presented at the Health Roundtable 2013 Innovation Workshops and Awards, November 8 2013.

14. Gajanayake, Randike, **Grunwell, Daniel**, and Sahama, Tony (2013) Empowering the Consumer through Accountable-eHealth (AeH) Systems. Presented at the Health Roundtable 2013 Innovation Workshops and Awards, November 7 2013.

Refereed Short Communications

15. **Grunwell, Daniel**, Gajanayake, Randike, and Sahama, Tony (2013) Improving usefulness of eHealth systems through Information Accountability. *e-Health Technical Committee Newsletter.*

Other contributions

16. **Grunwell, Daniel**, Sahama, Tony, & Gajanayake, Randike (2015) 2nd International Workshop on Secure and Privacy-Aware Information Management in eHealth. In 17th International Conference on E-health Networking, Application & Services (HealthCom2015), 14-17 October 2015, Boston, USA.

17. **Grunwell, Daniel**, Sahama, Tony, & Gajanayake, Randike (2016) 3rd International Workshop on Secure and Privacy-Aware Information Management in eHealth. In 18th International Conference on E-health Networking, Application & Services (HealthCom2016), 14-17 September 2016, Munich, Germany.

1 Introduction

In this chapter, I present the background for the research, an overview of the research problems addressed and contributions made, and an outline of the remaining chapters of this thesis.

1.1 Overview

eHealth refers to the use of the Internet as a communication medium in a health context (Pagliari et al., 2005). One of the main uses of eHealth information systems is for electronic health records (EHR) which contain comprehensive patient records shared by all healthcare professionals (HCPs) (Kahn and Sheshadri, 2008). Three major problems in today's healthcare environment are accessibility, quality, and cost (Hill and Powell, 2009). By making patient information easily accessible at the point of care through effective use of eHealth technologies, it is possible to reduce the number of medical errors from poor availability of patient information (Hill and Powell, 2009), which are responsible for a significant amount of hospital admissions (Williams, 2011). Having access and the ability to analyse the ever growing pool of health-related information will allow for better quality healthcare (Kwankam, 2004).

Shared eHealth records (SEHR), which I define as EHR systems that are shared among HCPs from different institutions such as national EHR systems, have the potential to improve healthcare by ensuring a high availability of information at the point of care and lowering costs of maintaining local EHR systems by HCPs (Hill and Powell, 2009; Yaffee, 2011). Australia now has a SEHR in place called the Personally Controlled Electronic Health Record (PCEHR) system, which allows consumers to opt-in to sharing online summaries of their health information with registered providers (Personally Controlled Electronic Health Records Act 2012, Clth; Department of Health, 2014). However, despite this potential the uptake of systems like

Australia's PCEHR system has been slow. The main reasons for this are claimed to be HCP dissatisfaction with the systems (Buntin et al., 2011) and patient concerns over privacy (Chen et al., 2010; Croll, 2011). Privacy in this context refers to the claim of individuals to determine when, how, and to what extent their information is used or disclosed (Westin, 1967). If privacy concerns can be adequately addressed, it will help to remove one of the barriers to the uptake of these systems, and as a result, help address the problem of accessibility of health information.

There are currently conflicting information access requirements between HCPs and patients in relation to access to information. HCPs desire prompt access to as much information as possible to make well-informed decisions, while patients want greater control over who can access their information and how it is used (Tierney et al., 2015). This conflict was highlighted in the recent review of Australia's national PCEHR system (Department of Health, 2014). For systems such as the PCEHR to reap the full benefits that such a shared EHR system can offer, an appropriate balance between the requirements of HCPs and patients must be met. In the current patient controlled model, HCPs are unable to rely on the SEHR as a complete source of information on a patient they are treating, and as a result, might be discouraged from using such systems (Liaw and Hannan, 2010; Garrety and van Teeseling, 2012).

To balance these competing requirements, the use of information accountability (IA), and specifically an Information Accountability Framework (IAF), in eHealth systems has been proposed (Gajanayake et al., 2012). We refer to eHealth systems that implement IA mechanisms as Accountable-eHealth (AeH) systems. Such AeH systems provide HCPs with non-restrictive access to information while empowering patients by enforcing transparency and accountability on the access to their health information. However, the IAF has yet to be implemented, and a study into the technical challenges and solutions of implementing IA protocols into eHealth systems is required.

1.1.1 Information Accountability Framework and Accountable-eHealth systems

The proliferation of eHealth, worldwide, is greatly hindered by information privacy concerns (Croll, 2011; Parks et al., 2011). Although healthcare information has been stored en masse in the past in the form of paper records, information privacy concerns seem more prolific in the modern electronic society; mainly because consumers have a perception that information stored in electronic form is more susceptible to misuse through external data breaches and internal rogue-users (Kierkegaard, 2011). These information privacy concerns are justified by events that have occurred in recent times with regards to EHRs in several countries. There have been numerous cases of patient privacy being breached by healthcare professionals and organisations either intentionally or through negligence, and in some cases the affected patients were not notified for a significant amount of time after the breaches were discovered (McCann, 2013b,c; Lieberman, 2012; McCann, 2013a; Hooper, 2012; CBC News – British Columbia, 2013b,a).

One of the major concerns is with 'insider threats', which include accidental disclosures, insider curiosity and data breach by an insider (Appari and Johnson, 2010). An insider refers to an authorised user of the system, such as a HCP in an eHealth environment. Insider threats are a serious concern for the privacy and security of patient data. Security in this thesis refers to measures to counter the unauthorised access, disclosure, or modification of information (Stamp, 2011). Approximately 18 percent of all health provider privacy breaches that were made public in the US between 2005 and 2015 were due to insider threats (Privacy Rights Clearinghouse, 2016). Misuse refers to the unauthorised access, use, modification, or disclosure of information, or other use of information that is not for the purpose for which the information was provided (Privacy Act 1988, Clth; Health Identifiers Act 2010, Clth). In Australia, health information may only be used in order to provide healthcare to an individual, and a small number of other limited purposes such as for approved research (Health Identifiers Act 2010, Clth).

In Australia, there have been reported high profile cases of insider misuse, such as a recently reported privacy breach where 13 staff members at a hospital in South Australia were found to have accessed the health records of the man accused of a high profile murder (ABC News, 2016; Toscano, 2016). External data breaches are often defended against using appropriate security protocols, which aim to prevent unauthorised entities from accessing the system. However, preventing data misuse by internal authorised users is a challenging undertaking. This challenge is further augmented in a complex domain such as healthcare. Although a purely preventive approach may be appropriate in many other domains, healthcare professionals cannot always be denied information that may hold the key to making a lifesaving decision. In fact, it has been shown that the lack of adequate information is a contributor to medication and clinical errors (Williams, 2011).

Information Accountability is a concept that involves using policies and mechanisms to encourage appropriate use through after-the-fact accountability for intentional misuse. IA mechanisms augment, but do not replace, traditional preventative measures that expect a user to be authorised to take an action in a system before doing so. The presence of IA mechanisms is intended to act as a deterrent for such misuse (Feigenbaum et al., 2011b).

The main goal of accountability systems is to be non-restrictive while maintaining accountability. By implementing non-restrictive access to information for legitimate users, AeH systems aim to fulfil the information requirements of healthcare professionals. Legitimate users are provided with the information they require for their job functions without rigid access restrictions. In an AeH system, the system provides disincentives for misuse by users in the form of accountability entailed by penalties (Feigenbaum et al., 2011b). These penalties would be defined and enforced by the governing body of the health system, such as a government health department or hospital board. It is expected that when users are aware of the accountability measures, they would not engage in inappropriate activities, much like in the offline world we live in (Feigenbaum et al., 2011a). Incentives are given to the users to follow the procedures and enforce appropriate use. Thus, AeH systems allow information to be made available to legitimate users more openly and effectively without threatening patients' information privacy. The knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives for patients to increase their trust in the system.

In previous work by Gajanayake et al. (2012), an initial model for an Information Accountability Framework for use in eHealth was devised. In the IAF model, patients are able to set usage policies on their HCPs' access to data rather than on their EHR items. For example, a patient may grant access for a particular HCP to view their EHR but restrict the HCP from viewing their mental health information. The presence of a Health Authority (HA) ensures that HCPs always have the access they need while respecting patient privacy requirements. The HA role would be fulfilled by the relevant administrator of the health system, such as a government health department. HCPs are able to access information they need without rigid barriers in order to provide care to their patient, while an accountability agent monitors for access requests for misuse. In the event a potential misuse of patient information is detected, the HCP is asked to justify their actions. A reasoner then makes a decision as to whether the justification is valid in the given context. Potential breaches are reported to both the patient and the HA so that the HCP can be held accountable for their actions if needed.

There have been previous approaches to applying IA to eHealth systems. Ferreira et al. (2006) proposed an access control model for EMRs that allowed doctors to "break the glass" and access any information they needed while providing non-repudiation for its access to provide accountability if this ability was misused. Seneviratne and Kagal (2014) proposed creating a new web protocol, accountable HTTP, that would provide provenance trails for the transmission of data and media on the web through a network of provenance trackers. Data owners would be able to set policies and audit the transmission of their information after-the-fact. Our approach includes aspects not present in previous approaches, including the role of a HA guaranteeing legitimate HCPs have appropriate access to the relevant information when they need it, the amalgamation of patient and HA policies, providing proactive detection and notification of potential misuse, and allowing patients to submit inquiries and interact with HCPs to resolve disputes. However, aspects of previous approaches could be applied in combination with the IAF protocols.

1.2 Research Problem and Contributions

Applying the IAF model to eHealth systems has been proposed as a possible solution to balance the patient privacy and HCP information access requirements (Gajanayake et al., 2012). In previous work, the concept of AeH systems was developed and an initial model of an IAF was devised using the results of survey responses that analysed the acceptability of an IA approach in eHealth. However, the proposed IAF protocols were not implemented. Through this research, we wanted to discover:

- How can the IAF and Accountable-eHealth systems be implemented?
- What are the requirements for implementing such systems?
- Are there gaps in the initial IAF model, and if so, how can they be addressed?
- What are the technical challenges associated with the implementation of Accountable-eHealth systems? How can they be solved?

Challenges that were investigated and solved in this research include:

- Analysing the security requirements for implementing the IAF protocols
- Extending the initial model of the Information Accountability Framework to allow for additional use cases including delegation of access
- Identifying and evaluating the usability requirements of AeH systems
- Identifying the requirements for the security and privacy of accountability mechanisms
- Exploring how the protocols can be implemented in existing EHR systems
- Investigating how the protocols can be applied to decentralised eHealth systems

The developed solutions to these challenges were evaluated and validated through simulations, scenarios, model checking, case studies, and user studies. A prototype of an AeH system using the IAF protocols was developed and used to explore the implementation and validate the functionality of the protocols. This research contributes to knowledge in the eHealth domain in terms of the implementation and use of Accountable-eHealth systems through:

- Identifying and exploring the requirements for the implementation of the IAF and AeH systems, particularly in terms of functionality, security, and usability
- Extending the IAF model to address identified gaps and provide support for more diverse use cases
- A validation of the feasibility of implementing the protocols in existing EHR systems and the identification of the requirements for such implementations
- Presenting a proposed approach to apply a modified IAF for use in decentralised systems

This work will determine how such systems can be practically implemented and demonstrate that the IAF model is mature enough to be implemented in existing EHR systems. Greater adoption of information accountability mechanisms in eHealth should lead to better delivery of healthcare services for the general public and the improved usefulness of shared eHealth record systems.

1.3 Thesis Outline

The rest of this thesis is arranged into the following chapters:

1.3.1 Chapter 2: Background and Related Work

This chapter summarises the background knowledge for eHealth, security and privacy, and accountability, and presents work related to this thesis.

1.3.2 Chapter 3: Designing Accountable-eHealth Systems

This chapter outlines the requirements for Accountable-eHealth systems and presents the initial architecture of the IAF. This architecture is used to define a threat model of both eHealth systems in general and the proposed IAF. I also discuss the IAF's place in the overall security of an eHealth system. The requirements and gaps in the current IAF model are used to expand and improve the model, and continue the investigation into the implementation of the protocols.

1.3.3 Chapter 4: Initial prototype implementation and user study

This chapter introduces, analyses and discusses an initial prototype implementation of the IAF protocols applied to a simple demonstration eHealth system. This prototype is used to demonstrate and validate the functionality of AeH systems.

When designing eHealth systems, usability must be a key consideration. As part of developing the IAF prototype, the requirements for the usability of AeH systems are discussed. The developed prototype was then used to perform a user study using a standard usability study method with the 'think aloud' protocol and a semi-structured interview. In this study, 20 participants filling the patient role used the prototype and provided feedback on the IAF protocols and the prototype's usability.

1.3.4 Chapter 5: Extending the IAF Model

This chapter focuses on expanding the IAF protocols to address gaps noted in Chapter 3. In particular, I present the requirements for enabling delegation of access in the IAF. The security risks associated with the accountability mechanisms are then discussed and the requirements for access to usage policies and provenance logs are defined. I modified the initial prototype discussed in Chapter 4 to accommodate these additional requirements.

1.3.5 Chapter 6: Implementing the IAF protocols into existing eHealth systems

This chapter discusses the implementation of the IAF protocols into two existing EHR systems, OpenEMR and FluxMED. It was found that the evaluated eHealth systems did not have existing accountability mechanisms that met our requirements. These implementations were used to demonstrate that it is possible to modify existing systems to support the IAF protocols and discuss the challenges of such implementations. The use of the two systems also enabled the exploration of two different approaches to implementing the IAF protocols. The implementations are compared and a small pilot study into the views of HCPs on the use of the IAF protocols is conducted using FluxMED.

1.3.6 Chapter 7: Applying the IAF to decentralised systems

This chapter discusses and explores the application of the IAF protocols for decentralised eHealth systems. A proposed model for the use of the IAF protocols in a decentralised environment is presented.

1.3.7 Chapter 8: Conclusion

This chapter concludes the thesis with a summary of the work, contributions, limitations, and future directions for the project.

1.4 Conclusion

eHealth systems promise many benefits in the delivery of healthcare. However, patient concerns over privacy and use of personal information and competing concerns from HCPs have hindered the acceptance of such systems. An Information Accountability Framework discussed in this thesis is one of the proposed solutions to these issues. However, the implementation of an IAF in an eHealth environment had not previously been investigated.

Accountable-eHealth systems enable the creation of shared eHealth records that can be useful to both consumers and HCPs. By ensuring transparency and accountability is applied, consumers are aware of how and why their information is accessed and used, while medical professionals are able to access all the information they need to provide care to their patients and make informed decisions. As a result, Accountable-eHealth systems create an eHealth environment where health information is available to the right person at the right time without rigid barriers, whilst empowering the consumers with information control and transparency, thus, enabling a means of reaping the full benefits from a shared eHealth record.

Accountable-eHealth system have the potential to balance the requirements of patients and HCPs, and enable improved healthcare through the high availability of clinical information. While the initial IAF model has been investigated for its acceptability by users, it had not yet been implemented and a number of challenges remain.

In the next chapter, I discuss the background and related work to the problem domains of eHealth systems with a focus on security, privacy, and information accountability in order to provide the basis for our work on the IAF and AeH systems.

2 Background and Related Work

In this chapter, I discuss the background and related work to the problem domains of eHealth systems with a focus on security, privacy, and information accountability. I present an overview of the current state of eHealth systems with particular regard to EHRs, the need for information accountability in current and future healthcare systems, and the issues related to information security and privacy in EHRs from the available literature.

2.1 eHealth

The term eHealth has been given various definitions, however, in general it refers to the combination of technology, public health and commerce (Oh et al., 2005). Currently, eHealth most often refers to the use of the Internet as a communication medium in a health context, differentiating eHealth from the broader field of medical informatics which includes the use of various technologies in the medical field (Pagliari et al., 2005).

The main use of eHealth information systems is for electronic health records (EHR) and electronic medical records (EMR). EMRs are patient medical records maintained individually by different HCPs, whereas EHRs are comprehensive patient records shared by all HCPs (Kahn and Sheshadri, 2008). The implementation of EHRs that can be accessed over the Internet could lead to significant cost savings for HCPs as they will have access to all of their patients' health information without having to invest in expensive EMR systems for their practices (Yaffee, 2011).

Three major problems in today's healthcare environment are accessibility, quality, and cost (Hill and Powell, 2009). Having easy access and the ability to analyse the ever growing pool of health-related information will allow for better quality healthcare (Kwankam, 2004). Evidence suggests medical errors resulting from poor availability of patient information are responsible for a significant amount of hospital admissions (Williams, 2011). Having patient information readily available can reduce these errors and lead to reduced costs through more effective healthcare (Hill and Powell, 2009).

EHRs enable improved quality of healthcare services to the general public by sharing access to structured medical data (Neubauer and Heurix, 2011). Many countries have been working on national shared EHR (SEHR) systems for some time now including the US, Canada, Australia, the UK, and throughout Europe (Cornwall, 2002).

It is generally understood that the adoption of EHRs and other eHealth technologies promise significant opportunities to improve healthcare (Buntin et al., 2011; Jha et al., 2009). However, the adoption of such technology by HCPs has not been as high as expected (Bramble et al., 2010; Jha et al., 2009). One of the barriers to the wide adoption of eHealth technologies is HCP dissatisfaction, with Buntin et al. (2011) pointing to the need for studies that identify the issues surrounding the implementation and adoption of EHRs and in particular into how they might be solved.

2.1.1 Information security and privacy in eHealth

Information security involves measures to counter the unauthorised access, disclosure, or modification of information, and information privacy refers to maintaining the confidentiality of an individual's personal information (Stamp, 2011). One of the most significant impediments to the wide adoption of EHRs is concerns regarding patient privacy and information security (Chen et al., 2010; Croll, 2011).

While there are varying definitions of privacy, in the context of this research, I refer to "privacy" in terms of the use and collection of information about an individual. A classic definition of privacy in this context is given by Westin (1967):

> “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” (Westin, 1967)

Information security likewise has varying definitions, but in this work I focus on a traditional definition of security involving three main objectives: confidentiality, integrity and availability (Von Solms and Van Niekerk, 2013). Confidentiality relates to the unauthorised access or disclosure of information. Integrity relates to ensuring the accuracy and completeness of data and preventing or detecting the unauthorised modification of information. Availability involves ensuring that information must be available when it is needed, which can be extremely important in a healthcare setting (Hill and Powell, 2009).

Security and privacy in EHR systems is vital as a patient’s health record contains sensitive information, the unauthorised disclosure of which can cause significant repercussions to the patient (Appari and Johnson, 2010). Sensitive information refers to information or opinions about an individual’s racial or ethnic origin, health or medical information, sexual preferences or practices, genetic information and other information as defined in Australia’s Privacy Act 1988 (Clth). Over time, EHRs can accumulate a complete profile of a person with information not directly related to treatment (Mercuri, 2004). As stated by Kierkegaard (2012):

> “The personal data available in health records is extensive. Health records include sensitive personal data or personally identifiable information such as medications, illnesses, medical records and history, sexual information, biometric information, hospitalizations, laboratory tests, substance abuse, allergies, drug interaction, messaging between providers (etc). Hospitals collect patients’ social security numbers, employment information, addresses, phone numbers, contact info, and religion. Besides information concerning the individual’s physical health, the health record

> may include information about family relationships, sexual information and physiological and mental health conditions, as well as the patient's private thoughts."

Although healthcare information has in the past been stored in the form of paper records, information privacy concerns seem more prolific in the modern electronic society; mainly because consumers have a perception that information stored in electronic form is more susceptible to misuse through external data breaches and internal rogue-users (Kierkegaard, 2011). The use of paper records is mainly governed by accepted ethical conduct of healthcare professionals and a data breach would be a physical loss of records or an act of vandalism. On the other hand, data in electronic form can be misused in a number of ways that may affect a patient's financial status, employability, insurability and harm their social status. These information privacy concerns are justified by events that have occurred in recent times with regards to electronic health records (EHR) in several countries (McCann, 2013b,c,a; Hooper, 2012; CBC News – British Columbia, 2013b). One particularly extreme case was in England in 2003 when it was reported that there was a serious breach of patient confidentiality at the Belfast Royal Victoria Hospital, resulting in the Real IRA gaining access to electronic patient records in order to gather information on police officers and politicians to target them for attacks (BBC News, 2003).

In their systematic literature review on information privacy concerns in EHRs, Rahim et al. (2013) identified nine factors that influenced information privacy concerns: trust in their HCPs; demographics (i.e. individuals with different backgrounds had different concerns regarding their privacy); the dissemination of their information (particularly when EHRs are exposed over the internet); computer literacy of both patients and HCPs; the inclusion of data patients consider sensitive in their EHR; the need for HCPs to get consent from patients over how their information is collected, used and who accesses it; the potential for a privacy breach; meeting legal and policy requirements in EHR systems; and the training of HCPs in EHR systems. The most prominent of these issues are concerns over information dissemination and computer literacy. As part of identifying these factors, common requirements in order to alleviate privacy concerns were identified including the need for a framework that can identify potential privacy breaches; having a proper mechanism to protect sensitive data; and making it transparent to a patient how their information is collected, transmitted, used and who it will be disclosed to both now and in the future (Rahim et al., 2013).

Concern over use of their information is one of the leading causes of reluctance from patients to opt-in to SEHRs. In addition to this, approaches to address privacy concerns by putting control of the information into the hands of patients result in HCPs being unable to trust that the information is complete. Patients desire the ability to control which HCPs can access their EHR and even the ability to prevent the viewing of specific health information by HCPs who have access to their record (Alhaqbani and Fidge, 2007; Tierney et al., 2015). For example, according to Alhaqbani and Fidge (2007) patients prefer to hide certain health information such as their sexual or mental health details.

HCPs, however, need easy access to as much information as possible in order to make well-informed decisions about their patients' well-being (Williams, 2011). In particular, emergency situations could require a HCP to override a patient's security settings in order to provide appropriate care (Ferreira et al., 2006; Tierney et al., 2015). Patient control of all access to their information is not appropriate in these cases, and many HCPs believe such restrictions would hinder the quality of care (Tierney et al., 2015). The ability to override patient preferences for access to information in certain situations is a requirement to providing appropriate care, and is essential in life-threatening emergency situations where HCPs may need to "break the glass" to access a patient's information. These competing requirements from patients and HCPs in EHR systems need to be balanced in order for such systems to be widely accepted (Gajanayake et al., 2013a; Tierney et al., 2015).

In Australia, the Personally Controlled Electronic Health Records Act 2012 (Clth) defines appropriate use and disclosure of health information, stating that the users, including HCPs, of the PCEHR system should adhere to the access controls set by the patient at all times when collecting, using and disclosing health information except in some circumstances as stated in the Act. Parts of the Health Identifiers Act 2010 (Clth) also handle the use and disclosure of health information.

A number of solutions to address privacy issues surrounding the adoption of EHR and SEHR systems have been proposed. In one such study, a context-aware access control model for assuring the privacy of medical records in an Internet-based open environment was proposed and recommended (Naqvi et al., 2010). Jin et al. (2011) proposed a unified access control scheme that allows the selective sharing of EHR information by patients using different levels of granularity. While there has been much research into defining possible EHR system security controls, Fernández-Alemán et al. (2013) found in their review of current work on EHR systems that these measures are not fully deployed in actual tools.

2.1.2 Shared eHealth Records in Australia and patient control

With the introduction of the Personally Controlled Electronic Health Record (PCEHR) system in 2012 (Department of Health, 2014), Australia now has a national SEHR system. However, as with eHealth in general, uptake has been slow. In their survey of attitudes toward the PCEHR, Lehnbom et al. (2012) found most consumers and HCPs identify that the benefits of PCEHR include instant access to healthcare information as well as safer and more effective healthcare delivery. However, the consumers involved in their survey were mostly unwilling to opt-in to the PCEHR, with breaches of privacy among the stated drawbacks.

The PCEHR, while an important step forward for eHealth in Australia, has not provided all the benefits a shared eHealth records system can offer. In particular, due to the characteristic implicit in the PCEHR, patients have total control over the information in their record. This is an issue from the perspective of HCPs, as explained by Liaw and Hannan (2010), due to individuals being able to "hide" information rather than "denying access" to their information in the PCEHR discourages HCPs from using a system where they cannot be certain of the completeness of the information. These features of the PCEHR were also criticised by the Australian Medical Association (AMA) who claimed that it was dangerous to give patients control over their medical information and thus the ability to restrict access to certain information and that it "could undermine all the potential benefits" of the system (Garrety and van Teeseling, 2012). Srur and Drew (2012) also point to the opt-in nature of the PCEHR as potentially leading to lower adoption rates and delaying the system's success.

The opposing needs of patient control and HCPs requiring access is highlighted in the Australian government's 2014 review of the PCEHR (Department of Health, 2014). The review noted that clinicians "warn about lack of confidence in the medical profession and the users of the system regarding the inability to be confident that the record has not been altered or that key information has been left out". Patients and privacy advocates were concerned about the safety and security of information and wished for consumers to retain control of their information. However, the recommendation of the report only moved to flagging information that a patient has restricted to the HCP who authored the information, but not to others. This conflict is still a concern for the value and success of the PCEHR, and a gap we believe can be filled with an IA approach.

Other recent studies have also identified this conflict in patient control of eHealth information, with Tierney et al. (2015) finding that while patients frequently preferred restricting HCP access to their EHR, HCPs believed that patients restricting access to EHR information would adversely impact patient care. They concluded that there is a need to balance these requirements. This is the goal of our work on the IAF.

While the potential of the PCEHR to improve quality healthcare and reduce clinical errors through instant access to information is high, the problems with the current implementation that decrease its usefulness and trust by both patients and HCPs must be addressed before it can realise its potential.

2.1.3 Access control in eHealth systems

As noted in Section 2.1.1, information contained in eHealth systems is often very sensitive in nature, and as such, it is vital that access to that information is appropriately managed. When implementing an EHR system, the security of the stored data, access control and access monitoring must all be considered (Rodrigues et al., 2013).

Access control consists of two key parts: authentication and authorisation. Authentication is the process of a user of the system verifying a claimed identity, for example using a password, key, etc., and authorisation refers to what users are allowed to do in a system (Stamp, 2011). The most prominent access control models for authorisation in eHealth systems are Role-Based Access Control, Discretionary Access Control, and Mandatory Access Control.

Role-Based Access Control (RBAC) involves making decision on access based on roles assigned to users within a system (Merkow and Breithaupt, 2014). Roles have associated permissions and as such permissions to perform actions or access resources are defined for all users of a given role, rather than specific to a given user. Roles are assigned to users in line with the requirements of the job within an organisation. Roles are also generally assigned in line with the principle of least privilege so that a user only has the minimum access they need to perform their job. RBAC is the most common access control model used in healthcare (Fernández-Alemán et al., 2013).

Discretionary Access Control (DAC) gives control of granting access to individual users. In a DAC mechanism, the owners of resources or information control which users have access. This is achieved through Access Control Lists (ACLs) such as file permissions on Operating Systems (Merkow and Breithaupt, 2014). However, on its own DAC has been proven inadequate in protecting sensitive health information in domains such as healthcare.

Mandatory Access Control (MAC) is somewhat opposite to DAC in that as opposed to individual users deciding which other users can access a resource, a central authority sets the access control policy. Access to information is restricted based on sensitivity labels such as "Secret" and "Top Secret" (Merkow and Breithaupt, 2014). For a user to access information, they must have a level of clearance that is greater than or equal to the classification of the resource. This is problematic in healthcare where a type of data may have different sensitivity levels for different patients, so a more flexible solution is required.

Another model is Purpose-Based Access Control (PBAC). PBAC involves relating data objects with purposes which are used to determine why the information was collected and what it can be used for (Byun et al., 2005). This approach has been found to provide greater privacy preservation for information (Byun et al., 2005; Yang et al., 2007; Ni et al., 2010), however, it also introduces a great amount of complexity to the access control mechanism (Al-Fedaghi, 2007). Despite this complexity, the concept of capturing why information was collected and what it can be used for is vital to protecting the privacy of sensitive health information.

An additional model that is sometimes used in healthcare is Attribute-Based Access Control (ABAC). ABAC involves using arbitrary attributes on the user and selected attributes on the object being requested to grant or deny access requests (Hu et al., 2015). This is a flexible approach that allows access rules to be defined without defining individual relationships between users and objects. The use of attributes on objects to determine access is useful, for example, a record could contain an attribute that it relates to sexual health history which could be used to determine access for HCPs who have an attribute of a sexual health specialist. However, for patient-controlled systems we must also link objects with specific users, rather than granting access to all users with a given attribute.

2.2 Meaningful use

“Meaningful use” is a concept that was included in the US government’s Health Information Technology for Economic and Clinical Health (HITECH) Act aimed at improving the quality of healthcare through increased quality, safety, and efficiency in EHR systems (Appari et al., 2013; Classen and Bates, 2011; Jha, 2010). A number of objectives and measures for assessing EHR systems in terms of meaningful use have been developed, including the need to implement systems to protect the privacy and security of patient data and enable the electronic exchange of key clinical information among HCPs (Blumenthal and Tavenner, 2010). These objectives can be used by countries implementing EHR systems to improve the quality of their healthcare (Gray et al., 2011).

The factors in achieving meaningful use that have implications for access control mechanisms include:

- implementing systems to protect the privacy and security of patient data (Blumenthal and Tavenner, 2010)
- enabling the electronic exchange of key clinical information among HCPs (Blumenthal and Tavenner, 2010)
- providing patients with timely electronic access to their health information

(Blumenthal and Tavenner, 2010)

- having the capability to generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach (Blumenthal and Tavenner, 2010)

- ensuring the system is usable and useful (Goldberg et al., 2011; National Institute of Standards and Technology (NIST), 2013; Zhang and Walji, 2011)

2.2.1 Implementing meaningful use

From the literature, four key aspects for implementing eHealth systems for meaningful use can be identified: usability, usefulness, utility, safety. These can be seen as strategies for implementing meaningful use.

- **Usability** – Usability refers to the ease of use of a system. It is an important, though often overlooked factor in achieving meaningful use and the adoption of eHealth systems (National Institute of Standards and Technology (NIST), 2013). Poor usability has been identified as one of the main causes of discontent and the slow rate of adoption with eHealth software (Belden et al., 2009; Classen and Bates, 2011). The usability of a system can have an impact on its security, usefulness and safety.

- **Usefulness** – Usefulness can be defined as the degree to which a feature of a system would improve or enhance a healthcare task (Keil et al., 1995). While the usability of a system is important, it is particularly important to design features that are identified as the most useful to also be highly usable (Schumacher and Lowry, 2010; Keil et al., 1995).

- **Utility** – Utility refers to the existence of a piece of functionality that is necessary to complete a specific task (Schumacher and Lowry, 2010). It differs from usability and usefulness in that it is simply a statement of whether it is possible to perform the task. Meaningful use regulation identifies a number of features, with the utility of a system being a measure of whether it implements all the required features. In terms of access control and information accountability mechanisms, the required features can be narrowed down to privacy and security measures, the ability to share or transfer information, and the capability to generate lists of patients by specific conditions while respecting the information privacy desires of the patients.

- **Safety** – Patient safety is a significant concern in EHR systems (Karsh et al., 2010; Classen and Bates, 2011). It is important the eHealth systems are designed to prevent errors such as providing wrong information to HCPs (i.e. errors in medication management). In access control mechanisms within EHR systems, it is also important for the safety of the patient that HCPs are allowed to override a patients' information access policies when necessary. If they were unable to do so, they may not have access to a key piece of information needed to treat the patient effectively, which could potentially cause errors in care. In many cases, safety has a strong connection to usability, as features that are not usable often lead to errors by users (Zhang and Walji, 2011).

2.3 Usability in eHealth systems

Usability is defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" (ISO 9241-11:1998, 1998). In an information system, it is a measure of the usefulness and ease of use of the system (Keil et al., 1995). Usability is a key factor in the acceptance of information systems by end users that must be considered from the early stages of development (Cysneiros and Kushniruk, 2003).

When designing eHealth systems, usability must be a key consideration. Belden et al. (2009) identified the lack of efficiency and usability as one of the key reasons for the slow rate of adoption of electronic medical records systems. Likewise, Classen and Bates (2011) point to usability as one of the most common sources of discontent among HCPs with vendor EHR systems.

As discussed in Section 2.2.1, usability is an important factor in achieving meaningful use in eHealth systems as it enables the effective, efficient, and safe use of such systems (Goldberg et al., 2011). If EHR systems are not usable, HCPs, patients and other users will be unable to benefit from many of the systems' features (National Institute of Standards and Technology (NIST), 2013). The usability in EHR systems can be measured based on how easy they are to learn, how efficient they are to use, error tolerance and user satisfaction (Zhang and Walji, 2011).

2.3.1 Usability and security

Usability and security are both essential components when designing an effective software system (Lang, 2011). However, they are often considered to be competing requirements (Lang, 2011; Garfinkel, 2005; Yee, 2004). In systems such as EHRS where users can be irrevocably damaged if the system is misused, breached, or data is inaccessible when it is needed, providing relevant usable security mechanisms is essential (Bonneau et al., 2015). Security mechanisms in systems should be easy to use, otherwise there is an increased chance that end-users will use the mechanism incorrectly or circumvent it in order to get their job done (Basin et al., 2011). Likewise, it can impact the motivation of users to behave securely if the security mechanisms increase the cognitive load of users through requiring them to remember or perform too many steps to act securely (Adams and Sasse, 1999; Beautement et al., 2008). Any possible conflicts between the security and usability goals can be avoided by considering both together throughout the design process of a system (Yee, 2004).

While the end users of a system are often considered to be the 'weakest link' in its security, Sasse (2005) point out that such issues are often caused by security mechanisms that are ineffective or hard to use. It is reasonable then to conclude that for an information system to be practically secure, its security mechanisms must also be usable.

Garfinkel and Spafford (1996) gave the following definition of a secure system: “A computer is secure if you can depend on it and its software to behave as you expect”. While this definition is broad, it brings up the point of thinking of security in terms of expected behaviour. In this case, we are considering expected behaviour for the end user of the system. Expected behaviour is also a key concept of usability design principles.

With an evolving understanding of the role of usability in security mechanisms, various research into appropriate methods to apply usability principles in the design of such mechanisms has been undertaken. Yee (2004, 2005) developed a set of guidelines for evaluating user interfaces of secure systems, focusing specifically on authorisation. These guidelines emphasise making the consequences of actions in a system clear to the user, and matching the most comfortable way of performing an action to the most secure.

Sasse (2005) worked on applying Human/Computer Interface (HCI) design methods when designing security mechanisms. In a related approach, Zurko (2005) focused on the concept of user-centred security, which refers to having usability as the main goal when designing a security mechanism or model. Flechais et al. (2007) introduced AEGIS, which defines a methodology for the development of secure and usable systems.

2.4 Decentralised systems and information sharing in eHealth

In addition to EHRs, there are an increasing number of heterogeneous distributed healthcare data sources that could provide additional information that could be used to drive clinical decision making and improve the quality of care (Marcos et al., 2015; Wood et al., 2015). These data sources can include sensor data obtained from monitoring patients and patient generated health data. This may be recorded by patients manually or collected by the various consumer devices (e.g. phones, smart watches, and fitness wristbands) and includes their vital signs, physical activity, sleep patterns, and medications (Wood et al., 2015).

With the large growth in health information from the variety of medical systems and sources, there comes significant issues such as interoperability and the creation of data silos (Richesson and Chute, 2015). With information commonly distributed among many hospitals and medical systems, a patient's health information is decentralised. To protect patient privacy, health data is often scattered and intentionally isolated among institutions (Weber et al., 2014).

If the various producers of this health information can be encouraged to share the data, there could be a significant increase the availability of the eHealth information at the point of care. In the US alone, it is estimated that healthcare data had reached 150 exabytes in size by 2011 (Cottle et al., 2013), and it is believed countries with large populations such as India and China could soon be handling zettabyte and yottabyte scale data (Andreu-Perez et al., 2015; Cottle et al., 2013). But while sharing patient information, we must ensure we address patient privacy concerns and provide mechanisms for patients to consent to their information being shared and used. Weber et al. (2014) states that there is a need for a consent mechanism that can enable patients to "decide how and when their data can be shared with or "mashed up" against other databases." This is a gap that a consent model for decentralised systems using Information Accountability protocols may be able to address.

2.5 Information Accountability

Traditionally, research into information security and privacy on the internet has focused on preventative measures such as authentication protocols and authorisation methods designed to prevent violations of policies by rigidly denying access to someone without appropriate permissions (Feigenbaum et al., 2012). However, using only this approach has proven inadequate for the increasingly complex requirements for data access and usage in various domains, and as a result more research has been completed into using Information Accountability (IA) mechanisms to augment preventive measures (Feigenbaum et al., 2011b).

While "accountability" is often given various and sometimes confusing definitions, Brinkerhoff (2004) identifies a general definition of accountability as:

> "...the obligation of individuals or agencies to provide information about, and/or justification for, their actions to other actors, along with the imposition of sanctions for failure to comply and/or to engage in appropriate action."

Information Accountability is an after-the-fact approach to information security that involves holding information users accountable for their actions through the application of policies so that any violations can be identified and potentially "punished" (Feigenbaum et al., 2011b). As such, Feigenbaum et al. (2011a) suggested the use of the word "deterrence" to better describe the general notion of IA systems. Feigenbaum et al. (2012) further clarify IA by stating that the term "accountability" does not just refer to anonymity, identification or exposure but also allows actions to be tied to consequences and violations to be tied to punishment. It is expected that when users are aware of the accountability measures, they would not engage in inappropriate activities, much like in the offline world we live in (Feigenbaum et al., 2011a). Key components for the implementation of IA are appropriate policy representation, policy aware transaction logs and policy reasoning (Weitzner et al., 2008).

Transparency of information use is critical to managing the increasing privacy risks associated with the exponential growth in communication, storage and search technology (Weitzner et al., 2006). Transparency and accountability allows potential misuses of data to be visible to all concerned (Weitzner et al., 2008). As such, transparency is a fundamental aspect of IA.

The importance and usefulness of IA in complex, information intensive domains such as eHealth is highlighted by Weitzner et al. (2008):

> "Information is widely available and the use of that information needs to be controlled. Rather than enforcing rigid up-front control over the use of information, there is a need to accommodate fair use. The control over the use of information is imperfect and exceptions are possible, but violators can be identified and held accountable."

When designing and implementing IA mechanisms to produce accountable systems, it is important to consider the design from a socio-technical perspective (Gajanayake et al., 2013b). A socio-technical system is one in which social and technical goals are interrelated (Cresswell et al., 2010). The implementation of an IA mechanism involves considering requirements from a technical perspective such as the implementation of the policies, logging, auditing, misuse detection, and information management; a socio-technical such as user acceptance, adoption, attitudes, capabilities, and meaningful use; and legal aspects such as information privacy, transparency, and accountability (Gajanayake et al., 2013b).

There have been various proposed approaches to implementing IA mechanisms. Jagadeesan et al. (2009) attempted to develop a formal foundations for the design of IA systems using privacy policies to define appropriate use of information. They focused on using audit logs which can detect potential policy violations and information misuse. Weitzner et al. (2008) proposed a transparent audit process that would track all transactions. Their proposal suggests the use of policies combined with policy-aware transaction logs and a policy-reasoning capability to enable accountable systems to hold users of information accountable. However, these studies generally focused on IA and accountable systems from a general point of view without consideration for the specific requirements of eHealth systems. Health is a complex domain and additional requirements for accountable systems must be considered to balance the needs of HCPs and patients.

In terms of IA in eHealth, Seneviratne and Kagal (2014) proposed creating a new web protocol, accountable HTTP, that would provide provenance trails for the transmission of data and media on the web through a network of provenance trackers. As part of evaluating the protocol, they implemented it for an EHR scenario where patients could audit the transmission of their information after-the-fact. This is a different approach to that taken by the IAF, which focuses on applying the IAF protocols to eHealth systems, allowing patients to set usage policies, providing proactive detection and notification of potential misuse, deterring HCPs from misuse, and allowing patients to submit inquiries through the system. However, this type of security protocol could potentially be applied in combination with the IAF protocols in AeH systems, providing an additional tracking mechanism for usage of medical data obtained throughout the web. Ferreira et al. (2006) proposed an access control model for EMRs that allowed doctors to "break the glass" and access any information they needed while providing non-repudiation for its access to provide accountability if this ability was misused. This is an essential step in providing safety through allowing access in emergencies with accountability in eHealth systems. However, this work only focused on break-the-glass circumstances. In the IAF, we want to also address accountability in all aspects of HCP access to information while providing patient management of access to their health data.

2.6 Provenance and Audit Logs

One of the key components of accountable systems are policy-aware transaction logs (Weitzner et al., 2008). These logs provide provenance of the data in the system. Provenance refers to the causal relationship between data and events that explains how it came to be in its current state (Miles et al., 2008). With the presence through such logs, the provenance of the data can be compared to usage policies to determine if an action complied with those policies (Aldeco-Pérez and Moreau, 2008).

Due to the central role audit logs play in accountable systems, it is crucial that they are correct and not alterable (Snodgrass et al., 2004). In such systems, it must be possible to detect if its logs have been tampered with in order to provide non-repudiable evidence of all actions (Haeberlen et al., 2007). Additionally, the provenance information in these logs can itself contain sensitive information that must be protected (Davidson et al., 2011).

While there has been some research in the area of preventing tampering of audit logs through cryptographic methods (Holt, 2006; Snodgrass et al., 2004; Haeberlen et al., 2007), the security and privacy issues surrounding provenance information is an ongoing challenge in designing accountable systems (Kagal, 2014; Hasan et al., 2007). Appropriate methods of securing and ensuring the integrity of these logs is an essential part of designing accountable systems.

2.7 Information Accountability in eHealth

Addressing patient information privacy concerns is crucial to the success of eHealth systems (Gajanayake et al., 2013a). While Information Accountability is not new, it is a relatively new and underexplored concept in healthcare (Gajanayake, 2013).

Requirements for access to eHealth information are inherently fine-grained. Access control to eHealth data often needs to be imposed based on the contents of the records, excluding some data while giving access to specific information (Chen et al., 2010). Because of this, traditional preventative security measures are not suitable on their own (Gajanayake et al., 2013a). The main aim of IA systems is to be non-restrictive, providing legitimate users access to information without rigid restrictions while imposing penalties for misuse of the information (Gajanayake, 2013). This is suited to the dynamic eHealth environment as restricting HCPs from accessing complete information on their patient can prevent them from being able to make fully informed medical decisions (Jolly, 2011).

2.7.1 Information Accountability Framework

IA mechanisms are particularly suited to balancing the competing requirements of patient privacy and HCP access to information, and to this end an Information Accountability Framework was proposed by Gajanayake et al. (2011). To define how IA can be used in eHealth systems, we must consider the main stakeholders:

- Patients
- Healthcare professionals
- Health Authorities (HA) (i.e. government health departments)

In an accountable-eHealth system, patients would be able to set usage policies on their HCPs, specifying which HCP should have access to which information in their health record. The presence of a HA ensures that HCPs always have access to the information they require through default access policies (Gajanayake et al., 2013a), and as such HCPs can trust that all necessary information is available to them if needed. HCPs will be able to access information needed to provide care to their patients in a non-restrictive manner, while being made aware of what information use is appropriate and the repercussions for misuse. As stated by Weitzner et al. (2006), all information access must be transparent to the subject of the information. As such, in an AeH system, logs of accesses to their information would be made

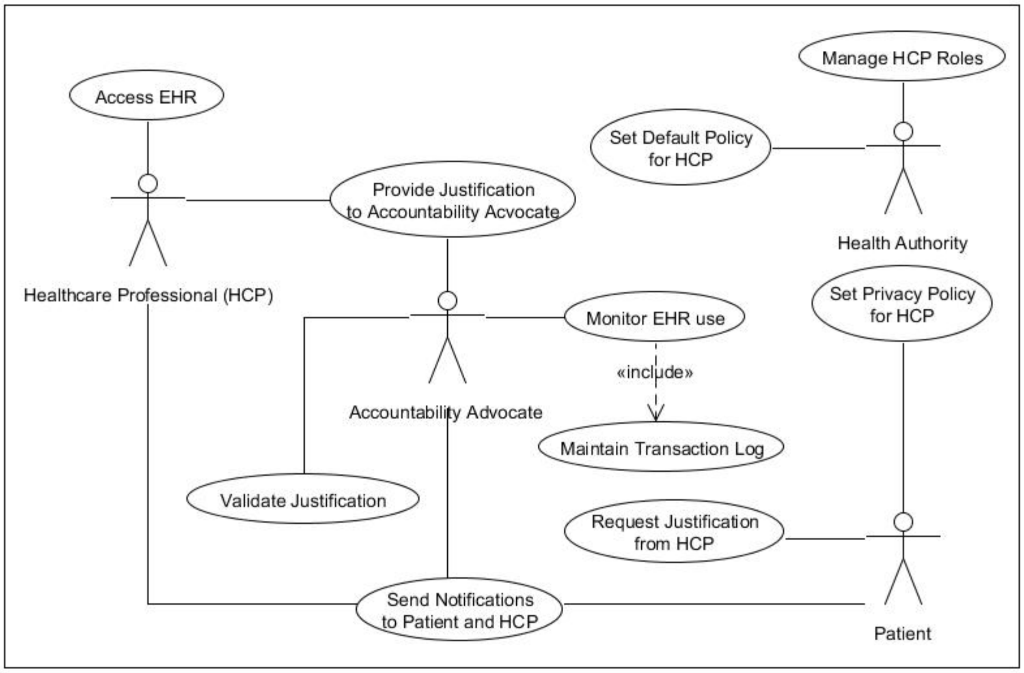

Access EHR
Manage HCP Roles
Set Default Policy for HCP
Provide Justification to Accountability Acvocate
Health Authority
Healthcare Professional (HCP)
Set Privacy Policy for HCP
Monitor EHR use
«include»
Accountability Advocate
Maintain Transaction Log
Validate Justification
Request Justification from HCP
Send Notifications to Patient and HCP
Patient

Figure 1: AeH model use case diagram (Gajanayake et al., 2012)

available to the patient. Patients should be able to query any potential misuse of information, with HCPs being required to justify their actions so they are held accountable. In addition, rather than just providing audit logs of information access, the proposed IAF would actively check audit logs, provide notifications of potential breaches to both the patient and HA, and provide patients with a user-friendly way to interact with these logs.

In the IAF proposed by Gajanayake et al. (2012), Digital Rights Management (DRM) technologies, specifically the use of the Open Digital Rights Language (ODRL) (ODRL Initiative, 2012), are used to represent the patient's usage policies. These policies are stored with the audit logs in order to provide context for a semantic reasoner to make decisions about potential misuse. The semantic reasoning process and the reasoning capabilities of the IAF have not yet been validated (Gajanayake, 2013).

Unlike the PCEHR system, in an AeH system patients do not have explicit control over their information; however, patients will still retain implicit control of their information through transparency of the actions of HCPs and the accountability measures put in place to assure appropriate use of information.

Figure 1 illustrates a simple use case of the Accountable-eHealth model proposed by Gajanayake et al. (2012). It illustrates the use of an accountability advocate that would use policies from the patient and HA to monitor for misuse by HCPs and validate provided justifications.

2.8 Conclusion

In this chapter, I have discussed the background and related work to the problem domains of eHealth systems with a focus on security, privacy, and information accountability. I presented an overview the current state of eHealth systems, particularly with regard to EHRs, the need for information accountability in current and future healthcare systems, and the issues related to information security and privacy in EHRs from the available literature.

The need to balance the requirements of patients and HCPs through appropriately augmenting existing access control and security mechanisms with an IA approach has been identified. The IAF protocols that have been proposed the potential to balance the requirements of patients and HCPs. We must explore the design and implementation of the IAF for use in eHealth systems to determine if the implementation of the theoretical proposal is possible and useful.

Section 2.4 also identified the need for a consent model in sharing and analysing information between organisations in a decentralised environment, a gap we believe the IAF can fill and will be discussed in Chapter 7.

In the next chapter, I discuss the requirements for an AeH system, explain the initial architecture and functionality of the IAF protocols in eHealth systems, define our threat model, and identify gaps in the initial model.

3 Designing Accountable-eHealth Systems

In this chapter,[1] I discuss the requirements for an AeH system and present the initial architecture and functionality of the IAF protocols in eHealth systems. I then define the threat model for the system to validate how the IAF protocols defend against threats from insiders and identify the risks associated with the initial IAF model. This analysis is also used to identify gaps in the model and extra requirements that need to be investigated and added to the model as we move towards an implementation of the IAF protocols in existing EHR systems.

The IAF's place in the overall security of an eHealth system is also be discussed, including the integration with other privacy and authentication/authorisation mechanisms and the respective requirements for such an integration.

3.1 Requirements for an AeH system

When designing and implementing the IAF protocols for use in an AeH system, we must consider various requirements including the needs of stakeholders in the system, as well as the security, usability, legal, and performance requirements of such a system. Addressing these aspects is necessary to implement a useful and usable eHealth system.

For eHealth systems to succeed, the needs of both HCPs and patients must be addressed. HCPs need to be able to access the relevant information in a timely manner, without rigid barriers. Patient control of all access to their information is not appropriate in these cases, and many providers believe such restrictions would hinder the quality of care (Tierney et al., 2015). The ability to override patient preferences for access to information in certain situations is a requirement to providing appropriate care, and is essential in "break the glass" emergency situations. An additional requirement from the perspectives of HCPs is the ability to share information with

[1] Publications related to this chapter: Grunwell et al. (2014); Grunwell and Sahama (2014, 2015b)

other HCPs in order to help make well-informed decisions.

In shared EHR systems where patients' private medical information is aggregated from multiple HCPs, patients should be able to determine who can access their EHR information. Additionally, patients have been found to prefer to restrict access to certain health information, such as their sexual or mental health information, from specific HCPs (Alhaqbani and Fidge, 2007; Tierney et al., 2015). Likewise, patients should have the ability to see how their information is being used and accessed. If patients are given the ability to manage access to their health information, the usability of the system used must be considered to ensure both that the system is used (Alhaqbani and Fidge, 2007) and that patients are able to understand how to manage their information and the consequences of changing the access to their record.

Due to the sensitive nature of medical information, the security of the system is a key requirement. Access to sensitive information must be restricted to only those that need it, so appropriate context-aware access control measures must be implemented. As discussed in Chapters 1 and 2, the goal of providing accountability is to deter misuse and provide transparency to use of information. In order to hold people accountable for their actions, a key requirement is the traceability of a user's actions in the system. This is a key concept that the IAF deals with. These security requirements, particularly in the context of the devised IAF, are discussed in more detail in Sections 3.3 and 3.4.

In managing sensitive information, there can be various legal requirements or standards that must be met by systems for them to be suitable for use in a given location. In Australia, the Privacy Act 1988 (Clth) defines principles that govern the retrieval, compilation, storage and use of personal information by agencies and organisations. Under these principles, any agencies or organisations that hold personal information must take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure (Privacy Act 1988, Clth). Health information falls under this act and is defined under “sensitive information” which includes information or opinions about an individual’s racial or ethnic origin, health or medical information, sexual preferences or practices, genetic information and other information. The Personally Controlled Electronic Health Records Act 2012 (Clth) and parts of the Health Identifiers Act 2010 (Clth) define appropriate use and disclosure of health information in Australia. While in Australia, health information is generally owned by the HCP who creates and manages the data, the Personally Controlled Electronic Health Records Act 2012 (Clth) provides more control of access to patients, stating that the users, including HCPs, of the PCEHR system should adhere to the access controls set by the patient at all times when collecting, using and disclosing health information except in some circumstances as stated in the Act. Parts of the Health Identifiers Act 2010 (Clth) also handle the use and disclosure of health information. If the IAF approach to provide less rigid access restrictions to ensure information is available when it is needed were to be implemented in the PCEHR, laws would be required to explicitly define how and why HCPs should be allowed to access health information.

Being transparent with people about how their personal information is handled is recognised as a fundamental privacy principle (OAIC, 2014) and must be a part of any policy around managing health information. Such transparency is essential in promoting trust among patients in how their information is handled, and is a key concept in IA. As part of ensuring this transparency, there is a need for a mandatory breach notification law in Australia to ensure patients are informed if their information is compromised and the recent draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Attorney-General’s Department, 2015) is a positive step in this direction.

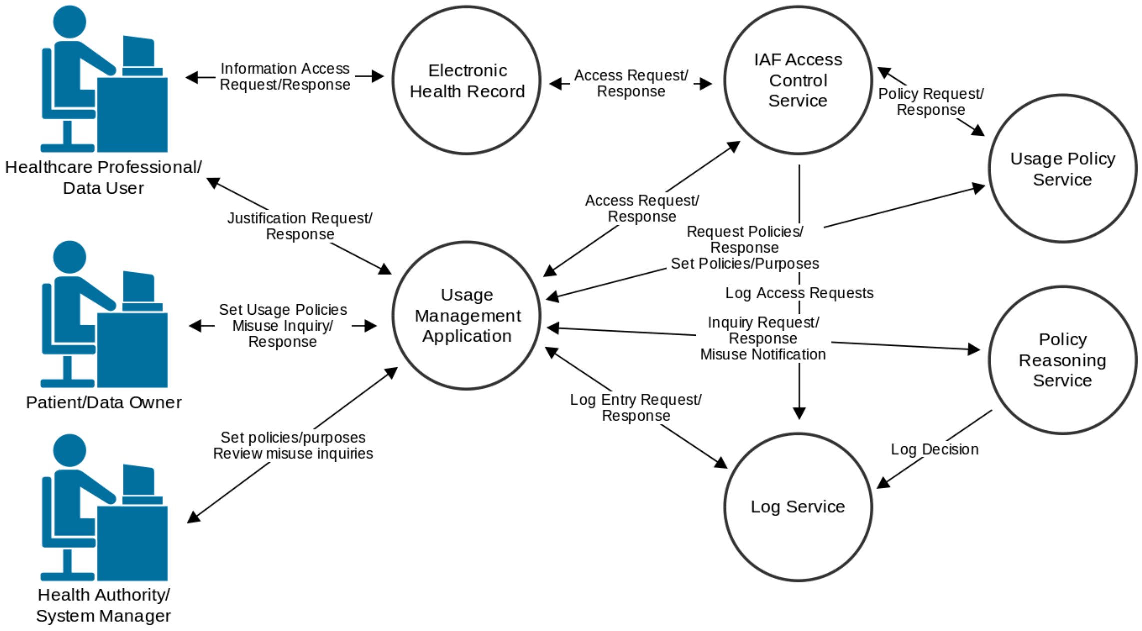


Figure 2: Proposed architecture of the IAF in an AeH system

For large scale eHealth systems such as a national EHR, the performance of the system is an important consideration. The system must be robust and scale to support growth in the number of users. This has security implications in terms of ensuring the availability of information, which is also discussed in Sections 3.3 and 3.4. When augmenting existing access control mechanisms with accountability, the performance of the IAF protocols must be considered to ensure they do not impact the availability of information when it is needed, regardless of the number of users.

These requirements are essential considerations in the implementation of an eHealth system. There is a need to balance HCP access requirements and the privacy and transparency requirements of patients in order for the full benefits of SEHRs to be realised. This is the problem the IAF protocols have been proposed to address.

3.2 Prototype Architecture of the Information Accountability Framework in an eHealth system

One of the goals of accountability systems is to be non-restrictive. Legitimate users are provided with the information they require for their job functions without rigid access restrictions. As a result, appropriate use of information is implemented, which is achieved by deterring users from intentionally misusing information. A fear of being caught is delivered with the presence of accountability mechanisms, which are appropriately conveyed to the users by means of internal messages. Incentives are given to the users to follow the procedures and enforce appropriate use. Accountability systems intend to increase consumer trust by implementing appropriate use and accountability measures.

By implementing non-restrictive access to information for legitimate users, AeH systems fulfill the information requirements of healthcare professionals. They provide disincentives for misuse to users which take the form of accountability entailed by penalties (Feigenbaum et al., 2011b). It is expected that when users are aware of the accountability measures, they would not engage in inappropriate activities, much like in the offline world we live in (Feigenbaum et al., 2011a). Thus, AeH systems allow information to be made available to legitimate users more openly and effectively without threatening patients' information privacy. The knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives for the subjects of the information, i.e. patients, to increase their trust in the system.

In defining the architecture for an AeH system implementing our IAF protocols, four types of users were considered initially: data owners (i.e patients), data users (i.e healthcare professionals) using health information for legitimate purposes, data users who misuse health information, and a central health authority (HA) (i.e. a government agency). In the IAF, data owners set information usage policies on their healthcare professionals, as opposed to assigning usage policies to assets. They are able to grant or limit access to their health information with a HA in place to guarantee that HCPs always have the access they need to provide appropriate care without hindering the patient's privacy.

Transaction logs of all activities on the system are stored. The entries in the logs contain information on whether the information access was policy-compliant, the date and time of the action, which HCP performed the action, and the context of the action (i.e. whether it occurred during a patient visit, emergency, consultation, etc.). However, in addition to providing audit logs of information access, an AeH system using the IAF actively monitors all actions taken in the system for potential breaches of policy. When a potential breach is identified, the AeH system provides notifications to both the patient and the relevant HA, as well as providing patients with a user-friendly way to interact with the logs.

If possible misuse of a patient's health information is detected by the system, the patient is able to lodge an inquiry asking for the HCP to justify their actions. The HCP must then provide an explanation that justifies their need to access the relevant information. While the HCP provides some initial context on the circumstances in which they need to view the information at the time of access, it was determined in the previous research and surveys conducted with patients and HCPs conducted by Gajanayake (2013) that HCPs having to provide a justification before they override a policy restricts their freedom to a certain degree. Gajanayake (2013) also found patients wanted the right to decide whether to inquire about possible misuse of their health information when a system notifies them of the event. Once the HCP provides a justification, the system then uses a policy reasoner with appropriate rules defined by a HA along with the context of the information access, usage policies, and the HCP's justification to determine whether misuse occurred and further investigation is required. If the system determines the justification provided by the HCP is not a valid reason to breach the patient's information usage policy, the HCP can be held accountable for the ramifications of their actions.

The initial proposed architecture I developed of an AeH system implementing our IAF protocols and the process flow between users and services is shown in Figure 2. The major components of the framework are the usage policy service, access control service, transaction logs, and the purposes reasoner. I use this architecture to develop an initial prototype in Chapter 4.

3.3 Threat Model

When designing secure software, a key step is the analysis of a threat model which can help identify the security requirements and potential threats and issues early in the process (Microsoft, 2016). In this section, I define a threat model for eHealth systems and explain how the IAF protocols aid in mitigating the identified risks, and identify the threats to an implementation of the IAF protocols.

3.3.1 Insider threats

Access control consists of two key parts: authentication and authorisation. Authentication is the process of a user of the system verifying a claimed identity, for example using a password, key, etc., and authorisation refers to what users are allowed to do in a system (Stamp, 2011). In developing the IAF protocols and working to integrate them into existing systems, we assume an appropriate authentication mechanism has successfully verified that a user is who they say they are. However, it is essential that such a robust authentication mechanism is in place. As the IAF is focused on holding authenticated users accountable for their actions within the system, the authentication system itself is currently out of scope of our work.

Our primary concern is with 'insider threats', which include accidental disclosures, insider curiosity and data breach by an insider (Appari and Johnson, 2010). Insider threats are a serious concern for the privacy and security of patient data, with approximately 217 (18%) of all health provider privacy breaches that were made public in the US between 2005 and 2015 being due to insider threats according to the Privacy Rights Clearinghouse. Insider breaches in this statistic were defined as “someone with legitimate access intentionally breaches information”. The number of such breaches was roughly equal to the number of breaches caused by physical loss of records, and significantly more than breaches caused by an outside party, malware or spyware (88 breaches). Accidental disclosures which is included in our definition made up a further 163 breaches bringing the number of breaches related to insider threats to approximately 30% of all breaches, though some these accidental disclosures included server misconfigurations (Privacy Rights Clearinghouse, 2016).

As noted in Section 3.1, Australia does not yet have mandatory public disclosure of data breaches so estimating the impact of insider threats in health data breaches in Australia is not possible. However, there have been reported high profile cases, such as a recently reported privacy breach where 13 staff members at a hospital in South Australia were found to have accessed the health records of the man accused of a high profile murder (ABC News, 2016; Toscano, 2016). This breach was caught months after the event during an audit of logs to check that only clinicians offering direct care of a patient were accessing records. This case highlights the value of a proactive monitoring and alerting of potential privacy violations, as well as the need to discourage such misuse through appropriate accountability mechanisms.

In dealing with insider threats, we assume the “attacker” in the scenarios I use to assess the IAF protocols is a valid, authenticated user in the system, with access to certain patient information. This patient information may include a patient’s full healthcare information in system as well as their address, birth date, and other personally identifiable information. In Australia, health information may only be used in order to provide healthcare to an individual, and a small number of other limited purposes such as for approved research (Health Identifiers Act 2010, Clth).

An attacker's abilities may also include the ability to modify or add to patient records in the system.

Insider threats could also include developers or others controlling the underlying software running the EHR system who could insert backdoors. However, we limit our focus to insiders who are valid users of the system, that is the data owners (patients), data users (HCPs), and administrators (HA).

3.3.2 Threat model for access to eHealth information

We can separate access to a patients eHealth information into two basic types: authorised and unauthorised. Authorised access refers to users such as healthcare providers who have been granted certain access to the healthcare information according to a set of access control policies enforced in the system. In looking at insider threats, we are concerned with attackers who fall into the group of authorised users. We can further split authorised access into proper or valid access to the information and improper access to the information which constitutes misuse.

In developing our threat model, I take a standard approach to threat modelling using aspects of the methods from Microsoft (Microsoft, 2016) and OWASP (OWASP, 2015). I followed the steps through the use of Microsoft's Threat Modelling Tool 2014 (Microsoft, 2014) to construct the threat model for an Accountable-eHealth system. This is used to help model and validate the effect of the IAF on insider threats. The steps involved are:

1. Identify security objectives/Vision

2. Diagram

3. Identify threats

4. Propose mitigations

Other similar threat models for insider threats and threats to health systems were used to compare the developed model and confirm the identified threats and mitigations (Shahri and Ismail, 2012; Kandias et al., 2011).

3.3.2.1 Identify security objectives/Vision

In the first step of the threat model development, the goals and vision for the threat analysis are explicitly defined. This allows us to focus the threat model in line with the goals of the system.

The main goal of the threat model is to identify the threats that could allow unauthorised misuse of patient health information by insiders and aid in identifying ways to minimise these risks. In using the IAF, we approach deterring misuse through the enforcement of usage policies and justification rules set by the HA and combined with usage policies set by patients.

3.3.2.2 Diagram

In the second step, a diagram of the application's architecture, components, and data flows are created. This allows us to understand how the main components, features, and users of the system interact.

To understand how the internal components of our system interact and how data is processed, I created a data flow diagram (DFD) of an AeH system making use of the defined IAF architecture. A separate DFD was created for each user flow because including all flows in one diagram would make the diagrams more difficult to understand and analyse. A high-level DFD of our AeH system for patients is shown in Figure 3, while Figure 4 shows the DFD for a HA user, and Figure 5 shows the DFD for HCPs. These diagrams show the flow of information between users, systems, and components. These model diagrams were created using Microsoft's Threat Modelling Tool 2014 (Microsoft, 2014). External entities are represented by rectangles, circles represent internal functions and services that will process data, two parallel lines represent databases or other data storage, and curved directional arrows represent the flow of data. Trust boundaries are represented curved dashed lines and refer to changes in privilege level.

3.3.2.3 Identify threats and propose mitigations

In the final two steps, the threats are identified that would compromise the security goals of the system defined in step one. Once these threats are identified, mitigations are proposed to address them.

In line with a standard definition of security as discussed in Section 2.1.1, we initially broke down threats to eHealth systems and information into three broad categories: confidentiality, integrity, and availability. A breach of confidentiality in an eHealth system could involve the unauthorised disclosure of a patient's health information, usage policies, log files, or any other restricted information stored in the system (International Organization for Standardization (ISO), 2014). A breach of integrity could involve any action that potentially leads to inaccurate or incomplete information in the system, such as the unauthorised modification or deletion of patient records, log files, or policies, or a HCP or other user being able to modify information without leaving a trace. A key part of integrity is non-repudiation, or the assurance that an event cannot be denied after-the-fact, and it is important that any system dealing with sensitive information provides for non-repudiation in order to provide accountability for misuse. A breach of availability could involve a security control preventing access to information when it is needed, service disruptions for various reasons including software or hardware failures, or a successful denial-of-service (DoS) attack.

In using the Microsoft Threat Modelling Tool, I used the STRIDE system for identifying and classifying threats to the system. STRIDE is mnemonic for security threats separated into six categories: spoofing of user identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege (Microsoft, 2005b). When evaluating a system using the DFDs created in step two, you work through each component and flow in the application and determine whether any threats for each STRIDE category exist (Microsoft, 2005a).

When assessing threats to access to eHealth information, I identify two core threats: unauthorised access to information and improper access to information or misuse. In this case, access refers to both the viewing and modification of information. These are primarily focused on breaches of confidentiality and integrity, but availability of information is also a key requirement for access to health information and is also one of the goals of the IAF in providing non-restrictive access to information when it is needed.

Unauthorised access to information could be accomplished by an attacker (who may or may not be an insider) through various means including stealing credentials from an authorised user (i.e. through social engineering, gaining access to a user database, etc.), use of an authorised users session (i.e. via an unattended laptop), or gaining direct access to (or stealing) a storage medium for the health information (such as a database, USB drive, etc.). This is caused by the attacker being able to bypass the relevant authentication method, and as a result, the success of an authorisation mechanism, such as the IAF protocols, are only successful if the authentication mechanism is robust. The IAF protocols do, however, provide a more fine-grained authorisation scheme that could limit the amount of information an attacker might gain access to, as compared to an RBAC approach where the assumed user may have access to a lot more information purely based on their role in the system.

An additional case of an unauthorised user accessing patient information through gaining access to an authorised account can be due to the sharing of an account or password. This may be done for various reasons such as allowing an assistant to enter patient data on behalf of a physician, or for a carer to manage access to the health record for a patient with a disability. In an accountable system in particular, it is essential that it is clear who is performing a given action so that they can be held accountable in the event of misuse, so accounts must not be shared. To address this threat, in Chapter 5 I extend the initial IAF model to include delegation of access to provide fine-grained means for an authorised user to grant delegated access to another user to act on their behalf.

Misuse of information involves insiders making use of their access for actions for which it was not intended. This is often possible in RBAC due to the same permissions often being granted to all HCPs of a given role such as “Physicians”, “Nurses”, or “Administrators”. The IAF protocols provide more fine-grained access to help address this. Firstly, patients maintain explicit control over who has access to their record, and as such, an insider can only access data on their own patients. Secondly, usage policies set by both the patient and the HA are used to restrict access to information that is not deemed necessary for the HCP to provide care to the patient. Thirdly, the provenance logging and proactive monitoring and notification of potential misuse of information provide after-the-fact accountability if misuse does occur. Messaging is used to convey the consequences of misusing information to a data user when they attempt to access restricted information. Ensuring the presence of the accountability mechanisms are known to act as a deterrent for misuse. Finally, *purposes* set by the HA are used to verify that the a justification given by a HCP for overriding a patient policy is a valid use of the information.

In the IAF itself, threats include the unauthorised viewing or modification of usage policies, purposes, and audit logs. The usage policies and audit logs of the patient’s eHealth information can themselves contain sensitive information that must be protected. Additionally, for the accountability mechanisms to meet the goals of holding users accountable for misuse, they must provide non-repudiation. I investigate this threat in more detail with explicit requirements for access and discuss solutions during implementation in Chapter 5.

Additionally, it is important that security and privacy management mechanisms are easy to use, otherwise there is an increased chance that end-users will use the mechanism incorrectly or circumvent it in order to accomplish their goals (Basin et al., 2011). In Section 4.4, I discuss the importance of usability in any security mechanism, and explore usable security design principles that apply to the IAF. I then conduct a usability study with users in the patient role in the system.

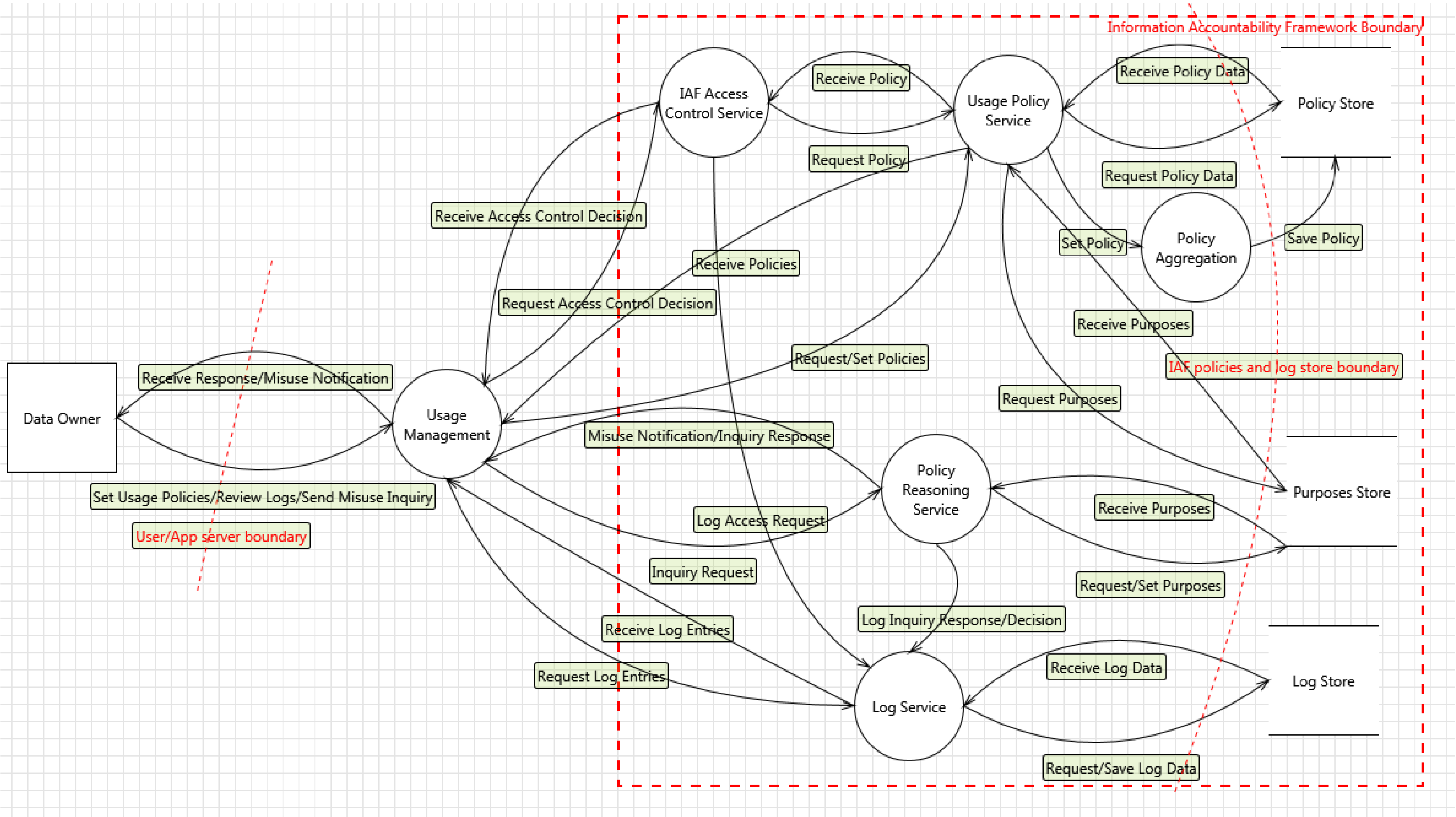


Figure 3: The flow of data within the IAF for data owners/patients

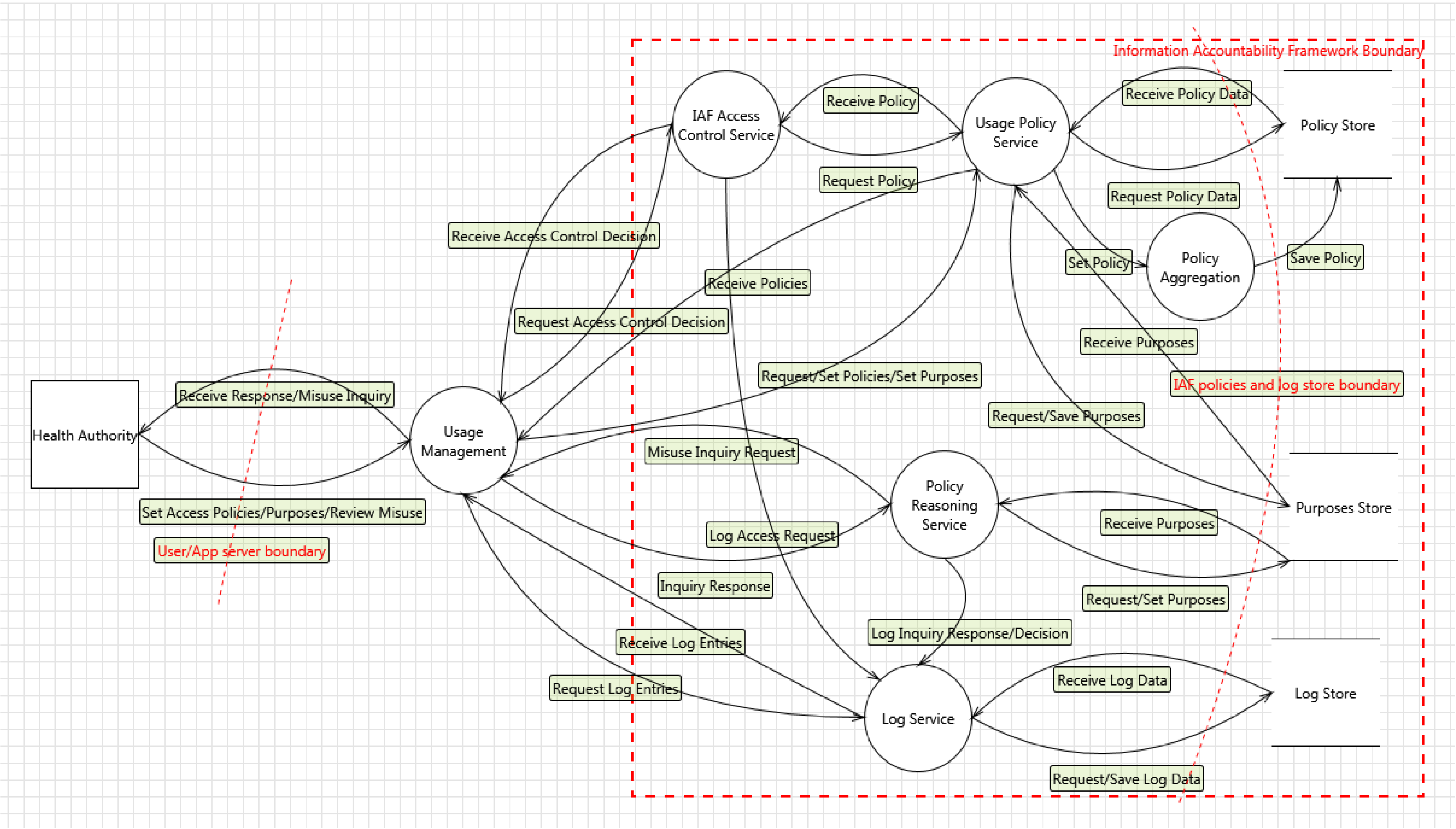


Figure 4: The flow of data within the IAF for the Health Authority

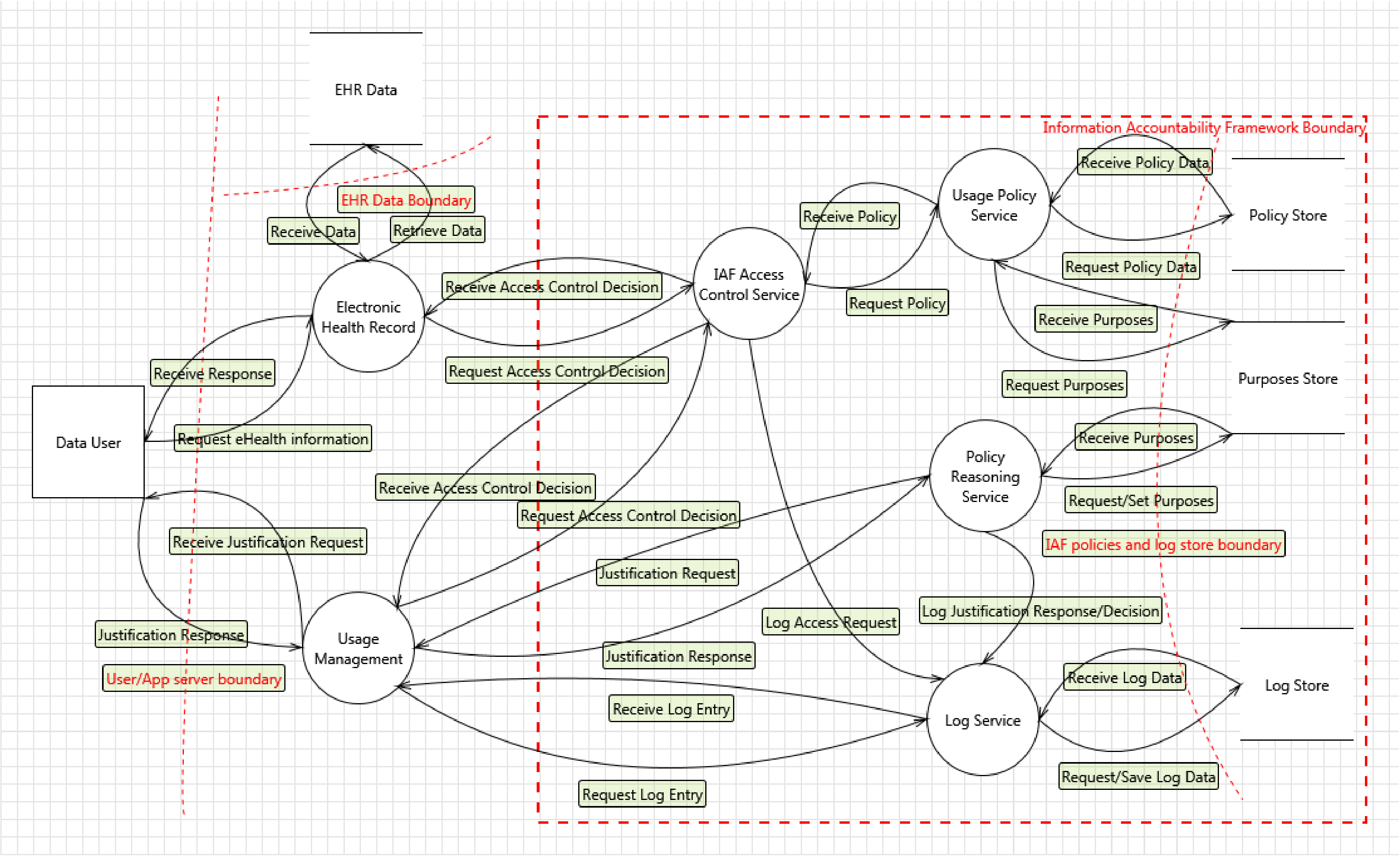


Figure 5: The flow of data within the IAF for data users/HCPs

3.4 IAF's place in the overall security of an eHealth system

The effective protection of health information and mitigation of insider threats requires a large number of countermeasures and defence in depth. The described IAF protocols augment, but do not replace, traditional preventative access control measures and it is important to consider the IAF's place in the context of an overall security system. In Figure 6, I show some of the possible security mechanisms in place in an eHealth system, with the IAF's role as part of the access control services and logging. In this section, I briefly highlight some of the main countermeasures we could expect in the overall security of an eHealth system and describe how the IAF fits in.

3.4.1 Security measures

Authentication: Accountability mechanisms are highly dependent on having robust authentication in place so that they can ensure non-repudiation. It is essential to have a robust authentication mechanism in place, represented in Figure 6 as "Multi-factor authentication".

Encryption: It is important to protect sensitive data both in transit and at rest, and previous work has recommended various approaches to encrypting eHealth records (Fernández-Alemán et al., 2013). However, such measures may not always be as effective against a malicious insider as they may have access to the data presented decrypted in the interface, or in the case of a network insider, may even have access to machines with the encryption keys.

Least privilege: The principle of least privilege involves limiting users to only have the access that is essential for them to perform their duties. This limits the impact a malicious insider can have in a given system. This is both useful as a general principle in a secure health system, but is also part of the IAF's role which involves restricting the types of information a HCP can access to only that which is required

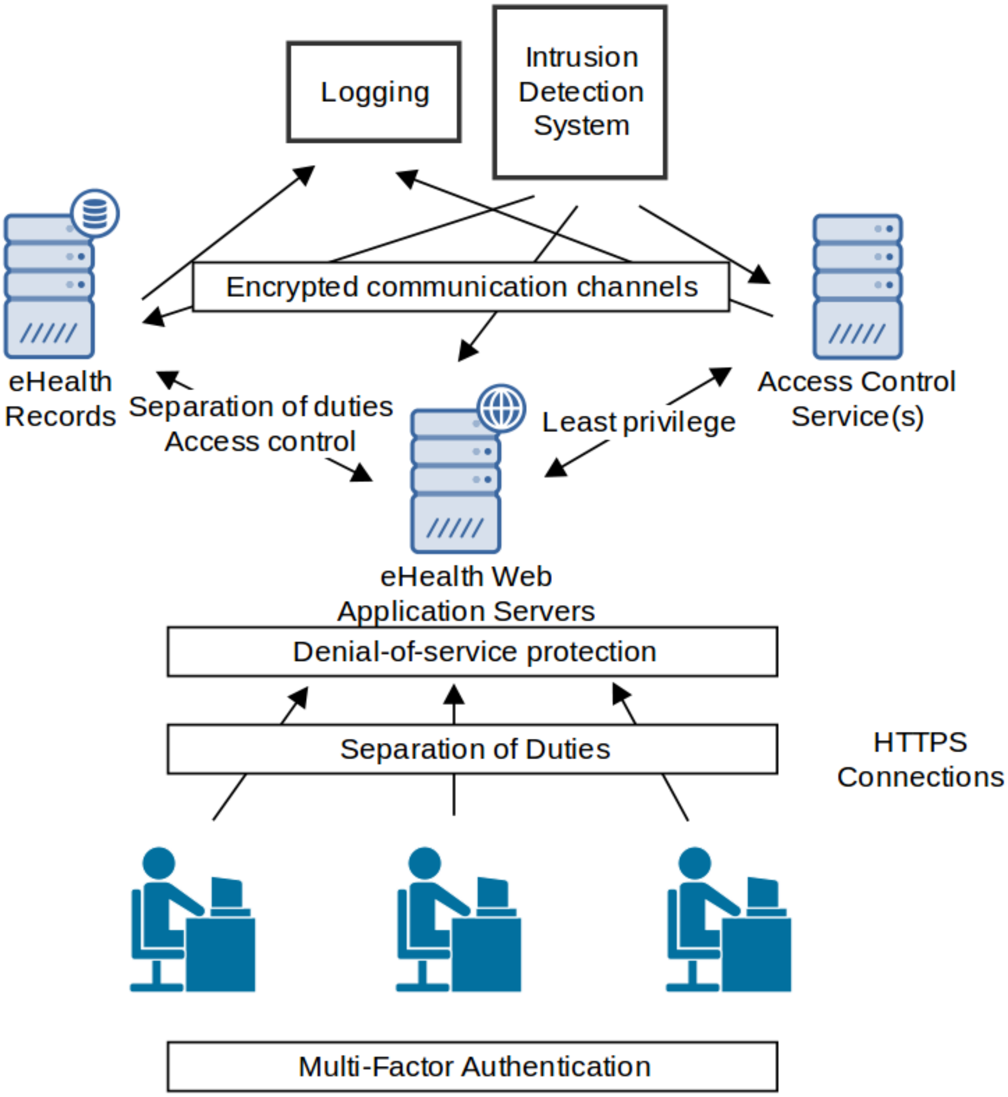

Logging
Intrusion Detection System
Encrypted communication channels
eHealth Records
Separation of duties
Access control
Least privilege
Access Control Service(s)
eHealth Web Application Servers
Denial-of-service protection
Separation of Duties
HTTPS Connections
Multi-Factor Authentication

Figure 6: Examples of security measures in an eHealth system

at a given time to provide appropriate care. However, being overly restrictive in providing access to health information can be detrimental to providing care. As a result, the IAF balances this by also aiming to ensure that HCPs can access the information they need without rigid barriers, while providing the means to hold them accountable in the event of misuse.

Separation of duties: Applying strict separation of duties (SoD), such as between HCP roles, system administrators, etc., can help limit the impact of an attack by an insider as the user will only have specific access based on their role and other business rules. In the case of the IAF, this includes usage policies. It also increases the likelihood of detecting an attacker attempting to escalate their privileges in the system.

Intrusion Detection/Prevention Systems: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are used to monitor network and system activity in an attempt to detect suspicious or malicious activity. Anomaly detection mechanisms are often used to identify malicious activity by monitoring for and identifying abnormal behaviour in the systems. In general, all systems that handle sensitive data in an eHealth environment should have IDS/IPS monitoring installed. There are also insider threat detection models that have been proposed that can be utilised to help detect various malicious behaviour by employees (Eberle and Holder, 2009).

Denial-of-service protection: As discussed in Section 3.3, it is essential to protect against breaches of availability to ensure that health information is available when it is needed. Protecting against denial-of-service attacks must be a concern for any Web-accessible EHR system, but is outside the scope of the IAF.

3.4.2 Integrating the IAF into an overall security of an eHealth system

In thinking about the integration of the IAF into the overall security of an eHealth system, we focus on the aims of the framework. The IAF aims to augment, but not replace, existing access control and other security mechanisms to provide accountability for misuse, act as a deterrent, and ensure the availability of information to the right person at the right time. In general, the IAF protocols will be integrated with the access control and logging mechanisms of a secure eHealth system. Through usage policies and purposes, the IAF provides more fine-grained separation of duties based on type of information and context of use, while also aiding in following the principle of least privilege. With the aims to provide accountability and deter misuse, the IAF targets malicious insiders who may be able to bypass other protections such as encryption and the use of an IDS.

For the goals of the IAF protocols to be achieved, a robust authentication mechanism must be in place that provides assurances that we know who is performing a given action. While the IAF itself focuses on authenticated users, the systems that directly store the private health information, including the usage policies and logs produced by the IAF services, must be secured through appropriate protections such as encryption of data, IDS and other monitoring, and DoS protections to ensure the availability of information.

3.5 Conclusion

In this chapter, I have discussed the requirements for an AeH system and the architecture and functionality of the IAF protocols in eHealth systems. A threat model for the system was defined and used to both help validate how the IAF protocols defend against threats from insiders and the risks associated with the initial IAF model. This analysis identified the need for additional requirements such as delegation of access and the need to protect the data stored and used by the accountability mechanisms. The missing pieces identified by the threat model are discussed in Chapter 5.

The IAF's place in the overall security of an eHealth system was also defined and discussed, including the integration with other privacy and authentication/authorisation mechanisms and the respective requirements for such an integration.

In the next chapter, I discuss the implementation of the initial IAF architecture as a prototype AeH system and use the prototype to analyse the functionality of AeH systems, assess the usability of accountability mechanisms, and perform a user study.

4 Initial prototype implementation and user study

In this chapter,[2] I first present my implementation of an initial prototype of the IAF applied to a simple demonstration EHR system. This prototype is used to demonstrate and validate the functionality of AeH systems. Throughout the rest of the thesis, this prototype is used as a base for experiments with the implementation of the IAF protocols. I then discuss the usability of the accountability mechanisms in the IAF. Usability guidelines for the design of AeH systems are identified and discussed, and the analysis of the initial prototype of the IAF is used to improve the prototype.

A user study of the improved prototype was conducted with 20 participants filling the patient role in the system, using a standard usability study method with the 'think aloud' protocol and a semi-structured interview. Participants in the study used the prototype and provided feedback on the IAF protocols and the prototype's usability.

4.1 Prototype implementation of the Information Accountability Framework in an eHealth system

I implemented a prototype of the IAF applied to a simple demonstration AeH system as a sample Web-based electronic health record system. The prototype system has functionality to allow patients to set access policies on their HCPs, review access logs for their EHR information, submit inquiries regarding potential misuse, and review responses from HCPs. It provides functionality to allow HCPs to access their patient's EHR information, and respond to patient inquiries into potential misuse by justifying their actions to the patient and the HA.

In this section, I describe the initial prototype's implementation. The major

[2] Publications related to this chapter: Grunwell et al. (2014); Grunwell and Sahama (2014, 2015b)

components of the prototype are the usage policy service and policy aggregation, access control service, transaction logs, and the semantic policy reasoner. Each of these components are detailed in this section.

4.1.1 Prototype technologies

Technologies that allow for quick iteration were initially used when developing the initial prototype, to allow for quick experimentation with the functionality and requirements of AeH systems. The prototype was first developed primarily using PHP (The PHP Group, 2016) and JavaScript, with a MySQL database (Oracle Corporation, 2016) as the primary data store for usage policies.

Upon further development of the prototype, the services of the IAF protocols were rewritten in Go, a programming language developed by Google for high-performance (The Go Authors, 2016), with the web application front-end remaining in PHP. The services that implement the IAF protocols are able to be reused by other eHealth applications and can be reused as needed when investigating implementing the protocols in existing EHR systems. The log storage backend that was chosen for the prototype was Apache Cassandra, a distributed database management system (DBMS) that is highly scalable and uses a distributed hash table (DHT) approach (The Apache Software Foundation, 2016). Usage policies were stored as quads, or named triples, and a graph database approach was taken to interacting with the policies to analyse the policies and rules. A few graph databases were experimented with including Cayley (Michener, 2014), and Neo4j (Neo Technology, 2016), which is the most popular graph database currently in use (DB-Engines, 2016). A graph database approach was used for our prototype rather than a relation databases like MySQL, as in the initial implementation, because it allows us to efficiently complex queries on ontologies, the relations between health data types, policies, rules, and users (Van Bruggen, 2014). Nginx (Nginx, Inc., 2016) was used to load balance the services so I could run multiple instances of each service to scale the system.

4.1.2 Policy representation

Developing an appropriate method to represent and manipulate usage policies is one of the main technical challenges when implementing AeH systems (Gajanayake et al., 2013a). With health information often spread among many health systems, interoperability of the systems is important in order to enable the effective exchange of health information (Hillestad et al., 2005). If health information is to be shared among systems and institutions, being able to understand the usage and information sharing policies presented by a system is essential. In our designed IAF prototype, we made use of an Open Standard Digital Rights Management (DRM) technology as a solution to this problem. There are a number of DRM policy languages such as the Extensible Access Control Markup Language (XAML), Enterprise Privacy Authorization Language (EPAL), and the Open Digital Rights Language (ODRL). We chose ODRL (ODRL Initiative, 2012) to represent information usage policies in our framework because it is independent of implementation constraints and is capable of expressing a wide range of policy-based information. While XACML is useful for fine-grained attribute-based access control, ODRL is particularly useful for broader policy-based control and supports concepts like duties (obligations), which is useful for our needs. However, it is possible to represent the policies required in XACML with appropriate changes if needed.

4.1.3 Usage policy service and policies aggregation

The usage policy service handles the retrieval, storage, and aggregation of usage policies. In our proposed system design, data owners can change the usage and access policies of their preferred HCPs. Through an interface they can restrict access to specific areas of their EHR, such as sexual health or mental health data. Patients are

```xml
<o:policy xmlns:o="http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov
   " uid="policy-use-ehr" conflict="prohibit">
  <o:permission>
    <o:asset uid="urn:ehr:12318" relation="o:target"/>
    <o:party uid="urn:patient:12318" role="o:assigner"/>
    <o:party uid="urn:healthPro:sexualHealth:10946" role="o:assignee"
       />
    <o:action name="o:read"/>
  </o:permission>
  <o:prohibition>
    <o:asset uid="urn:ehr:12318:mentalHealth" relation="o:target"/>
    <o:party uid="urn:patient:12318" role="o:assigner"/>
    <o:party uid="urn:healthPro:sexualHealth:10946" role="o:assignee"
       />
    <o:action name="o:read"/>
  </o:prohibition>
</o:policy>
```

Listing 1: An example access policy represented in ODRL

able to control which HCPs should be able to access which information. However, default policies set by the HA ensure that the required access levels are always given to the appropriate HCPs without unnecessarily impeding the patients' privacy requirements. To accomplish this, the system aggregates the patient's policy with the HA policy for that HCP to produce an amalgamated policy.

When the policies are being aggregated, there may be conflicts between the patient policy and the default policies set by the HA. For example, a patient policy may restrict access to sexual health history for a dermatologist, while the HA policy may grant the dermatologist access based on the relation between dermatology and sexual health. The access levels (AL) of a given HCP can be represented as tuple of what they can access, followed by what they cannot, with denial of access taking precedence. So, to say Dr. S can access all of the EHR, but not access sexual health and mental health history, this could be represented as:

$$AL_{Dr.S} =< [EHR], [SexualHealth, MentalHealth] >$$

A HA policy will generally focus on specifying what must be accessible by a HCP, so a dermatologist Dr. S may have the following HA policy:

$$AL_{Dr.S} =< [Dermatology, SexualHealth], [NULL] >$$

When aggregating these policies, a conflict would exist on access to sexual health information. In these cases, the general rule is that patient policies take precedence when granting more access to information, but the HA policy will take precedence over a restriction in a patient policy to ensure HCPs always have access to the information they need. However, rules can be defined to determine whether this should be the case for all types of information. As such, the resulting access for Dr. S after amalgamating the policies would be:

$$AL_{Dr.S} =< [EHR], [MentalHealth] >$$

Listing 1 shows an example representation of a policy for a sexual health specialist's access to a patient's record that gives them access to the patient's EHR while restricting their access to the patient's mental health history. In this policy representation, a permission is granted for the asset "ehr:12318" which refers to the health record for the patient with ID 12318. A prohibition is set for the mental health data in the health record as represented by the asset "ehr:12318:mentalHealth". This policy has been created by the patient represented by the "assigner" entry for "patient:12318" and the policy is assigned to the HCP with an ID of "healthPro:sexualHealth:10946". The "action" determines what the permission allows and prohibition disallows, which in this case refers to the ability to read the health record. The conflict attribute shows that there was a conflict between the patient's and the HA's policies where the patient tried to restrict access to information the HCP required to provide appropriate care. By keeping track of conflicts in the amalgamated

```
<o:policy xmlns:o="http://odrlextension.org/ns/odrlx/2x" xmlns:eh="
   urn:ehealth.gov" uid="policy-use-ehr" conflict="prohibit">
  <o:permission>
    <o:asset uid="urn:ehr:12318" relation="o:target"/>
    <o:party uid="urn:patient:12318" role="o:assigner"/>
    <o:party uid="urn:healthPro:sexualHealth:10946" role="o:assignee"
       />
    <o:action name="o:read"/>
  </o:permission>
  <o:prohibition>
    <o:asset uid="urn:ehr:12318:mentalHealth" relation="o:target"/>
    <o:party uid="urn:patient:12318" role="o:assigner"/>
    <o:party uid="urn:healthPro:sexualHealth:10946" role="o:assignee"
       />
    <o:action name="o:read"/>
  </o:prohibition>
  <o:transaction uid="transaction-use-ehr" valid="true" type="
     generalUse" dateTime="20130901112233"
    location="urn:emrlocation.org/10946">
    <o:asset uid="urn:ehr:12318" relation="o:target"/>
    <o:party uid="urn:healthPro:sexualHealth:10946" role="o:user"/>
    <o:action name="sexualHealth/patientVisit"/>
  </o:transaction>
</o:policy>
```

Listing 2: A transaction log entry represented in ODRL

policy, we can make it clear to the patient that the HCP will still be allowed to access information they tried to restrict access to. Likewise, the AeH prototype gives a warning to HCPs accessing such information that the patient prefers they did not view that part of their EHR, allowing them to take extra care to inform their patient of why they require access to that information.

4.1.4 Provenance logs

A key component of the AeH system is context aware logging of information accesses. In the prototype, all information access by HCPs is logged. Relevant summaries and details from the logs are made available to patients. When an invalid access request is made, the patient is notified of the potential misuse of their eHealth data, and they will be able to review all the access logs for their EHR.

Log entries contain information on which HCP accessed the data, the date and time of the access, the context of the request (patient visit, consultation, etc.), and whether the access was policy-compliant. The interface provides options for the patient to either mark invalid access requests as OK, if they are satisfied the HCP was not misusing their information, or submit an inquiry requesting the HCP justify their actions.

Listing 2 shows an ODRL representation of a log entry. It contains the policy shown in Listing 1 in addition to the context of the event and whether the access was valid and policy compliant. The context of the event is in this case a patient visit to a sexual health specialist, as represented by the action "sexualHealth/patientVisit", that occurred on the 1st of September, 2013, as recorded in the "dateTime" property. It is important that all log entries store the usage policy as it was at the time of information access, in order to provide the patient and the reasoner with appropriate context for deciding whether there may have been misuse.

The transaction log service is responsible for retrieving, storing, and verifying provenance log entries. The logging service is primarily interacted with by other services within the overall IAF service. Log entries stored by the IAF are context-aware and as such log entries contain information on which HCP accessed the data, the date and time of the access, the context of the request (patient visit, consultation, etc.), and whether the access was policy-compliant. The security concerns around provenance logs produced by the IAF protocols are discussed in both Section 3.3 and Chapter 5.

4.1.5 Access control service

When HCPs attempt to view entries in a patient's EHR, a request is made to the Access Control Service which then compares the access request with the patient's

EHR access policy. The Access Control Service sits between the EHR data and the user. It has the role of enforcing the patient's access policies. It makes use of the aggregated policies and the context of the request provided by the HCP to determine whether the access to the patient's information should be permitted. Regardless of the decision, data on all requests is sent to the logging service. For entries the HCP is permitted to view, they are immediately presented with the information. The access will be logged as valid and no notification will be sent to the patient.

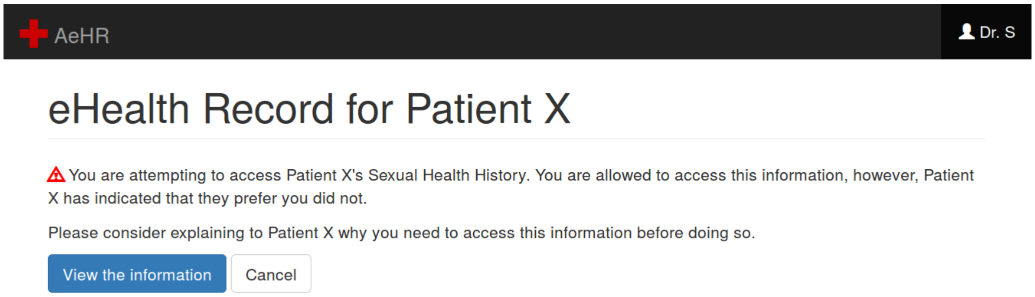
However, if the service determines that they are not allowed to access that particular piece of information, a warning will be displayed that provides the HCP with the option to view the entries, stating that their access to that information is necessary. If they continue on to view the entries, the access request will be logged as invalid and a notification will be sent to the patient so they can review the details and inquire about potential misuse.

4.1.6 Reasoner

The reasoner step makes use of policies, log entries, and rules defined by the HA for what constitutes appropriate use in order to make a decision about whether a reason for breaching a policy was justified. This occurs when a patient submits an inquiry and the HCP responds with a justification.

When a patient submits an inquiry into a potential misuse of their data, the relevant HCP is notified and is required to respond to the inquiry and justify their actions. The response must include a reason as to why they superseded the patient's access policy and accessed data that they were not allowed to.

When the HCP responds, it is run through a reasoner, which makes use of rules defined by the HA along with the information stored in the log entry to determine whether the HCP's response is an appropriate reason to override a patient's access policy. The reasoner takes into account the type of data accessed, the HCP's role,



eHealth Record for Patient X

⚠ You are attempting to access Patient X's Sexual Health History. You are allowed to access this information, however, Patient X has indicated that they prefer you did not.

Please consider explaining to Patient X why you need to access this information before doing so.

Figure 7: Warning screen when an access policy conflict exists

the context under which the information was accessed, and the reason provided by the HCP.

In the prototype, the HCP selects from predefined reasons to simplify the analysis, however, future work could make use of natural language processing to allow more verbose responses from HCPs. They are also able to enter a comment that will be visible to patients, communicating their reasons.

If the reasoner determines the HCP's response is valid, the patient will be notified of this and given the option to request an investigation by the HA if they are not satisfied by the response.

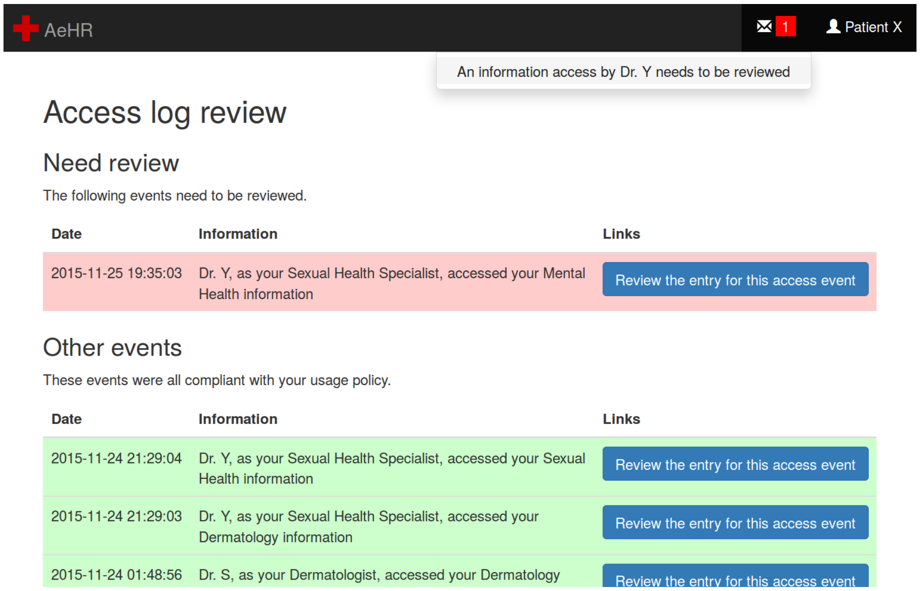
If, however, the reasoner determines that the response is not valid, the HA will be notified to investigate the situation to determine if any misuse has occurred. The patient will also be notified that the access will be investigated by the HA.

4.2 Case Scenarios

In testing the implemented prototype, a number of expected scenarios were developed to demonstrate the functionality of the AeH system. In this section, I describe four such scenarios that demonstrate different hypothetical situations and outcomes.

The scenarios involve the following characters:

- **Patient X**: Our protagonist. This patient has two different HCPs they see for different specialisations.



An information access by Dr. Y needs to be reviewed

Access log review

Need review

The following events need to be reviewed.

Date	Information	Links
2015-11-25 19:35:03	Dr. Y, as your Sexual Health Specialist, accessed your Mental Health information	Review the entry for this access event

Other events

These events were all compliant with your usage policy.

Date	Information	Links
2015-11-24 21:29:04	Dr. Y, as your Sexual Health Specialist, accessed your Sexual Health information	Review the entry for this access event
2015-11-24 21:29:03	Dr. Y, as your Sexual Health Specialist, accessed your Dermatology information	Review the entry for this access event
2015-11-24 01:48:56	Dr. S, as your Dermatologist, accessed your Dermatology	Review the entry for this access event

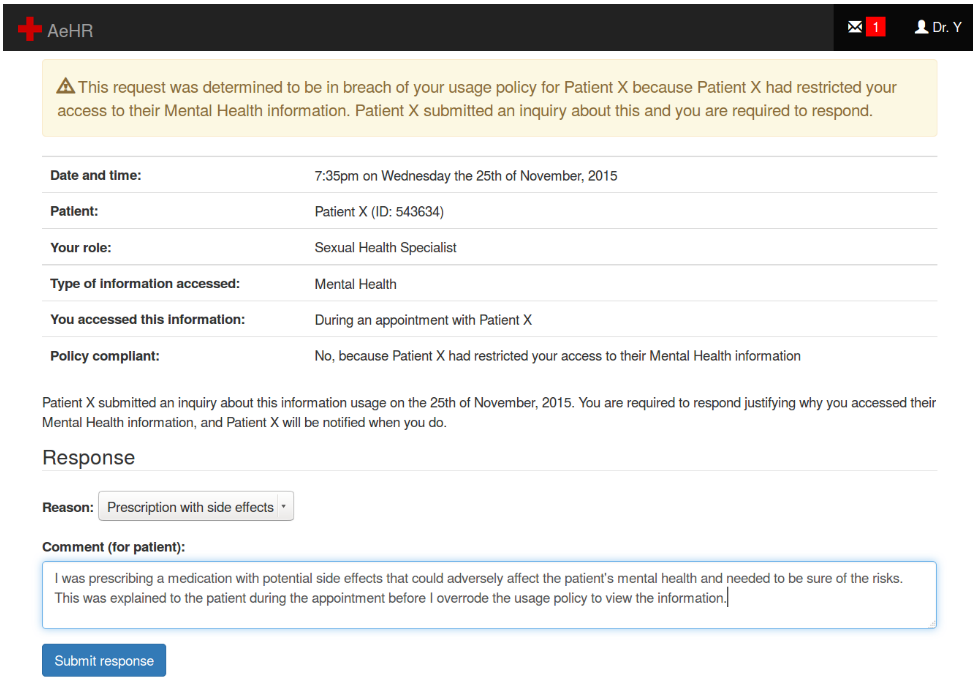
Figure 8: Patient's EHR access log

- **Dr. S**: Patient X's dermatologist. Patient X has given them access to their EHR but restricted Dr. S's access to their sexual and mental health information. However, the HA has set a policy requiring that dermatologists have access to sexual health information due to the relation between the two fields.

- **Dr. Y**: Patient X's sexual health specialist. They have been given access to Patient X's EHR but have been restricted from accessing the patient's mental health history.

4.2.1 Scenario 1 – Valid access with conflicting policy

In Scenario 1, Dr. S accesses Patient X's EHR during a visit to their office. They access the patient's dermatology history and, due to the nature of the patient's issue, sexual health history. When accessing the patient's sexual health history, Dr. S is notified that the patient had set a policy preferring that their sexual health history was not accessed. Seeing this, they explain to Patient X that the skin issue is related to a sexual health related condition, and so a review of their sexual health records is necessary to provide adequate care. This complies with the patient's access policy,



⚠ This request was determined to be in breach of your usage policy for Patient X because Patient X had restricted your access to their Mental Health information. Patient X submitted an inquiry about this and you are required to respond.

Date and time:	7:35pm on Wednesday the 25th of November, 2015
Patient:	Patient X (ID: 543634)
Your role:	Sexual Health Specialist
Type of information accessed:	Mental Health
You accessed this information:	During an appointment with Patient X
Policy compliant:	No, because Patient X had restricted your access to their Mental Health information

Patient X submitted an inquiry about this information usage on the 25th of November, 2015. You are required to respond justifying why you accessed their Mental Health information, and Patient X will be notified when you do.

Response

Reason: Prescription with side effects

Comment (for patient):

I was prescribing a medication with potential side effects that could adversely affect the patient's mental health and needed to be sure of the risks. This was explained to the patient during the appointment before I overrode the usage policy to view the information.

Figure 9: Dr. Y responding to the patient's inquiry

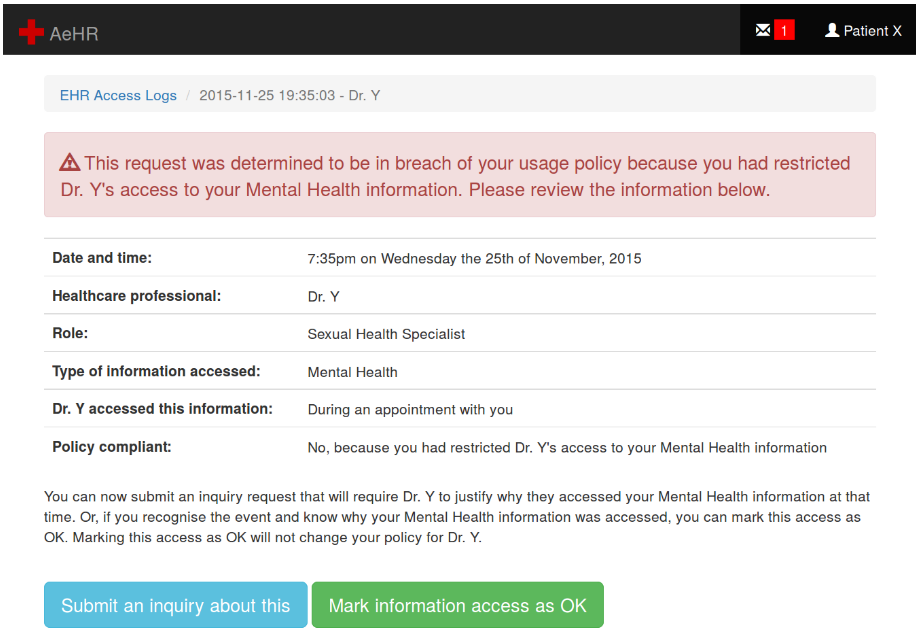
so the access is logged as OK with no active notification to the patient.

Figure 7 shows the warning screen Dr. S would see before being allowed to access Patient X's sexual health records.

4.2.2 Scenario 2 – Valid inquiry response

In Scenario 2, Patient X, who believes they may have contracted an STD, visits Dr. Y. During the consultation, Dr. Y accesses the patient's sexual health information, which is policy-compliant. However, during the consultation, Patient X begins to suffer from a mental breakdown. Forced to take some action, Dr. Y overrides the patient's access policy and views their mental health history attempting to identify any information that can help in the situation. As this action breached the policy, it is flagged for review by the patient as shown in Figure 8.

Sometime later, the patient submits an inquiry to Dr. Y to explain why their mental health information was accessed. Dr. Y responds with a reason that describes the mental breakdown the patient suffered during the consultation. The reasoner



EHR Access Logs / 2015-11-25 19:35:03 - Dr. Y

⚠ This request was determined to be in breach of your usage policy because you had restricted Dr. Y's access to your Mental Health information. Please review the information below.

Date and time:	7:35pm on Wednesday the 25th of November, 2015
Healthcare professional:	Dr. Y
Role:	Sexual Health Specialist
Type of information accessed:	Mental Health
Dr. Y accessed this information:	During an appointment with you
Policy compliant:	No, because you had restricted Dr. Y's access to your Mental Health information

You can now submit an inquiry request that will require Dr. Y to justify why they accessed your Mental Health information at that time. Or, if you recognise the event and know why your Mental Health information was accessed, you can mark this access as OK. Marking this access as OK will not change your policy for Dr. Y.

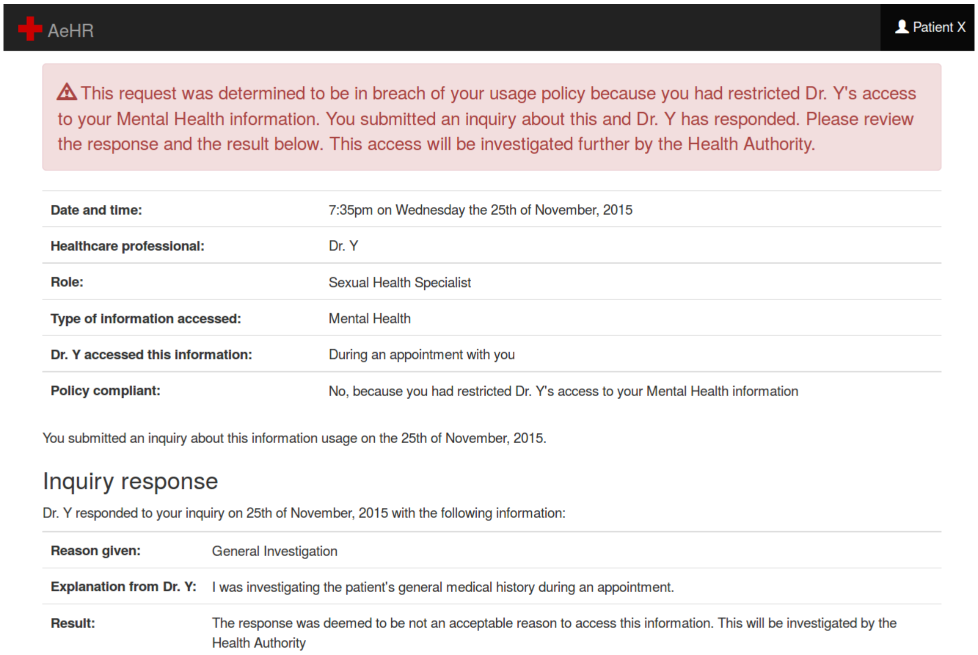
Figure 10: Access log summary entry

determines this to be a valid reason to override the patient's policy on mental health information and notifies the patient of this decision.

4.2.3 Scenario 3 – Invalid inquiry response

In Scenario 3, Dr. S is treating Patient X for a skin condition and notices behaviour that makes him concerned about the patient's mental state. Curious, he accesses the patient's mental health history, overriding the patient's policy to do so. As this is not a policy-compliant information access, the AeH system notifies the patient of this event for review.

Patient X reviews the log entry for the access and, concerned as to why Dr. S would have needed to view his mental health history, submits an inquiry from the interface shown in Figure 10. Dr. S responds to the inquiry, stating that the information was for use in providing general healthcare for the patient. The reasoner determines that this is an invalid reason for Dr. S to override a patient's policy and access their mental health information, and notifies the HA. The patient is notified



⚠ This request was determined to be in breach of your usage policy because you had restricted Dr. Y's access to your Mental Health information. You submitted an inquiry about this and Dr. Y has responded. Please review the response and the result below. This access will be investigated further by the Health Authority.

Date and time:	7:35pm on Wednesday the 25th of November, 2015
Healthcare professional:	Dr. Y
Role:	Sexual Health Specialist
Type of information accessed:	Mental Health
Dr. Y accessed this information:	During an appointment with you
Policy compliant:	No, because you had restricted Dr. Y's access to your Mental Health information

You submitted an inquiry about this information usage on the 25th of November, 2015.

Inquiry response

Dr. Y responded to your inquiry on 25th of November, 2015 with the following information:

Reason given:	General Investigation
Explanation from Dr. Y:	I was investigating the patient's general medical history during an appointment.
Result:	The response was deemed to be not an acceptable reason to access this information. This will be investigated by the Health Authority

Figure 11: Access log summary after an invalid response from Dr. Y

of this outcome, with a message informing them that the event has been reported and will be investigated as a breach of privacy as shown in Figure 11.

4.2.4 Scenario 4 – Challenging an inquiry response

In Scenario 4, Dr. Y has been provided with incentives from Patient X's insurance company to provide them with information on the patient's health record. The insurance company wants to have the full details of the patient's medical history before giving them a policy, and makes a deal with Dr. Y as one of Patient X's HCPs. Dr. Y accesses the patient's EHR, including their mental health history, to collect information to send to the insurance company. They give the context of the information request as being made during a patient visit.

As Dr. Y has not been granted access to this information by the patient, the system notifies the patient of a potential misuse of their data. Upon reviewing the access log entry, the patient submits a request for a response from the HCP justifying their need to access that information. Dr. Y, in a further unethical act, lies in the response, stating it was for the purposes of deciding on a possible prescription for the patient's recent treatment that had potential mental health side-effects.

Under the rules specified by the HA, the system determines this reasoning to be probably valid, so the patient is notified of the response for review. Upon reviewing the Dr Y's response, the patient realises the time of the information access does not match up to their recent appointment and Dr. Y had said no prescription was necessary. They submit a request for investigation into the HCP's response from the HA by simply clicking the relevant link in the log review interface.

4.3 Performance evaluation

The IAF is intended for implementation into large systems like national eHealth systems. As such, the performance of the system is important. It needs to be robust and able to scale to support the growth in number of users of such systems. An initial evaluation of the performance of the implemented prototype was performed.

Due to the limitations in not being able to simulate a large scale eHealth system at this time, I focused on benchmarking the prototype for the initial evaluation. The primary goal of the evaluation was to assess the overhead that the IAF adds to requests for access to health information. The most common requests to the IAF are expected to be checking if access to a given piece of information in a record is allowed, and adding associated logs when the information is accessed with the given permission, and as such these requests were the focus of the benchmarks.

The test involved generating policies for one million patients which were randomised to having between one and ten HCPs for different purposes (GPs, dermatologists, psychiatrists, etc.). Then a load testing tool called Locust (Locust, 2016) was used to define HCP user behaviour and then swarm the system with many simultaneous users requesting patient information. The simulated HCPs were associated with patients that they had permission to access so I could define their behaviour in requesting information in the patient's record. Locust was configured to make one request per second using a random HCP requesting a relevant record.

The IAF services were situated on another machine on the same network as the service making requests. Both machines were consumer grade hardware, which was a limitation as I was not able to evaluate the prototype's performance in a realistic environment at this time.

I compared the performance of retrieving information from the example eHealth system with and without the additional checks and requests to the IAF service.

It was found that the IAF service adds an average overhead of 164ms to the request for health information in the prototype under the simulated load. Given that this was conducted on consumer hardware, a consumer network, and performance optimisations such as tuning the DBs, appropriate cache layers, etc. are possible, this overhead can be considered acceptable in the context of healthcare and requesting information while providing care. The actual results may differ in implementations in different eHealth systems, depending on the extra processing they need to perform to interact with the IAF protocols.

In future, I recommend that a full performance evaluation is performed on an implementation in an existing eHealth system by making use of replicated traffic from the users of the system.

4.4 Usability

As discussed in Section 2.3, it is important to consider the usability in addition to the security of a system throughout its design. In order to implement the IAF protocols and AeH systems, the usability or ease of use of the accountability mechanisms must be considered. In this section, I explore how the features of AeH systems can be designed to meet usability principles.

4.4.1 Usable Accountable-eHealth systems

From the usable security design principles described by Yee (2004), Sasse et al. (2001), Zurko (2005), and others, the following simple design principles have been identified and applied to our AeH system:

1. It must be clear to the patient what authority other users (i.e. the HA and HCPs) have over the patient and their resources (i.e. healthcare information)

2. The result of changing authorisation levels for the resources a patient owns must be transparent to the patient

3. The most straight forward way to perform an action in the system should match the most secure method

4. It must be clear to a data user (HCP) when their actions may breach a patient or HA policy

5. The consequences of the HCP's actions within the system must be clearly conveyed to the HCP

In this section, the major components of an AeH system implementing the IAF protocols are discussed with recommendations for implementing these design principles.

4.4.1.1 Defining and aggregating usage policies

In our IAF model, patients are able to set information usage policies on their HCPs. They can for example grant their General Practitioner access to their health information but restrict them from viewing their sexual health history. In addition to these patient defined policies, the HA sets default policies on what information HCPs should be able to access. The patient policy and HA policy are amalgamated to produce an overall policy for the HCP who the patient has granted access to their EHR, with conflicts resolved based on predefined rules.

When a patient using an AeH system is setting usage policies on their HCPs, the system must make it clear how to restrict access to information that is important to them in accordance with Principle 3. For example, when first developing the prototype, patients were able to configure access to all information for every HCP. This led to a difficult to use interface, so it was redesigned to only show the types of information relevant to that HCP. Likewise, applying Principles 1 and 2, upon saving a new policy it must be clear to the user which information will be accessible by a given HCP and when. Clear messaging is important, particularly when presenting conflicts to the user. If a user's policy conflicts with the HA policy, the result of amalgamating those two policies must be transparent to the user.

It is important that users of an AeH system know what they can control in terms of who can access their information. If users find they are unable to rely on what they perceive to be controllable, it can lead to lower trust in the system and have a significant negative impact on the adoption of such an information system (Sasse, 2005).

As an example, when the HA has specified minimum access for a particular HCP and the patient policy conflicts with this access requirement, the interface of the system must make it clear to the patient that the HCP will still be permitted access to this information. By making the resulting access policy clear to the patient we increase the transparency of the system, which can increase user trust in the system. This can have a positive impact on user satisfaction, which is a key measure of the usability and usefulness of a system (Zhang and Walji, 2011).

In implementing an AeH system, the usability of the interface for editing information usage policies is a significant security concern. For example, if the HA accidentally gives too much default access to patients' health information, sensitive patient data could be accessed without alerting the patient or the HA. Likewise, a patient could accidentally grant access to information they would prefer was private. In the cases of both the HA and patient, we cannot assume the individual making the change is particularly computer-savvy. The risk of users misunderstanding a piece of functionality or making a mistake while using the system can be lessened by increasing the usability of the AeH system. The chance that the HA or patient will inadvertently grant too much access to a patient's health information could be reduced by making the user confirm any access policy changes on a screen that highlights what information the changes will grant access to.

Usable systems should be capable of helping users prevent and recover from errors (Zhang and Walji, 2011). In changing access policies in AeH systems, errors can have a serious impact on the security and privacy of patient data, and so interfaces to IA mechanisms must be easy to learn and must aid the user in preventing errors.

4.4.1.2 Accessing patient information

In the AeH prototype, when a HCP or other authenticated data user attempts to view entries in a patient's EHR, the access control service compares the context of the access request with the amalgamated usage policy for that HCP. If the HCP is permitted to view an entry, they are immediately presented with that information and the access is logged as valid with no further action. However, if they are not permitted access to that particular piece of information, the HCP will see a warning that will give them the option to view the entries, stating that their access to that information is necessary (an example use of this may be in an emergency). If they do access such information, the action will be logged as invalid and a notification will be sent to the patient with details of the access request so that they can review it and submit an inquiry about potential misuse.

In addition to this, when a conflict exists in the amalgamated policy, where the patient may have tried to restrict access to information that the HA has specified that the HCP must be able to access to provide care to the patient, the HCP will be informed via a warning as depicted in Figure 7 so that they can take additional care with the information and proactively explain to the patient why they need access.

In accordance with Principle 4, the design of the AeH must make it hard for the HCP to unknowingly breach a patient's policy. Likewise, per Principle 5, it must be clear to the HCP when a particular action may be in breach of patient's information usage policy and the potential consequences of that action. This can be achieved through the use of clear warning/confirmation screens prior to an action that may breach a policy.

4.4.1.3 Determining if misuse has occurred

One of the key components of accountable systems are context-aware transaction logs (Weitzner et al., 2008). These logs provide provenance of the data in the system. Provenance refers to the causal relationship between data and events that explains how it came to be in its current state (Miles et al., 2008). With the presence of such logs, the provenance of the data can be compared to usage policies to determine if an action complied with those policies (Aldeco-Pérez and Moreau, 2008).

In the AeH prototype, all access to a patient's information is logged and made available to the patient in a user-friendly format. A patient can review access logs at any time, but when an event that breaches a policy occurs they are notified to review the log entry for that event and can submit an inquiry requesting the HCP justify their actions. When the patient reviews the information in the log entry, they have option to submit an inquiry or mark the action as acceptable.

When an inquiry is submitted, the HCP is required to respond, justifying why they needed to access the relevant information. Once the response is submitted, a semantic reasoner uses the context-aware log entry and rules defined by the HA to make a decision as to whether the provided reason is an appropriate reason to override the usage policy. If it determines the reason is valid, the patient is informed of the result and is provided with an explanation for accessing the information. If, however, the information access is determined to be inappropriate, the HA is notified so that the situation can be investigated and handled in a predefined process, and the patient is informed that the situation is being investigated.

For patients, it is important that the process for how they can ensure their information hasn't been misused is intuitive and transparent. Likewise, when the result of an inquiry is communicated to the patient, it is important to make the reasons the semantic reasoner arrived at the specific conclusion clear. The patient is actively notified when they need to review an event in the system. When reviewing a log entry, they are given two simple options to either submit an inquiry or mark the event as OK. By keeping this process simple and making the next steps for the patient clear the design will be in keeping with Principle 3.

For HCPs, it must be easy to justify their actions accurately. They should not feel like they could be investigated for potentially misusing patient information if they have done nothing wrong but misunderstood how to use the system. The system must make it clear to the HCP the correct method and format to enter their justification. This can be accomplished through a structured form that makes it clear what information is required, as opposed to free text entry that could make the requirements for the justification unclear to the HCP.

4.5 User study

In order to assess the usability of the implemented IAF protocols, a qualitative user study was devised using standard usability testing protocols. In the study, users actually use the implementation of the protocols and provide their perceptions on managing access to their information using IA protocols.

The study involved a set of participants who performed in the patient role in the system. For the purposes of the initial study, the target number of participants was 20.

4.5.1 Ethics and Limitations

This study was conducted with approval from the QUT Human Research Ethics Committee (approval number 1500000920). The study was considered low risk and no ethical issues or incidents arose while conducting the study.

The IAF is a proposed approach to managing access to health information in EHR systems, and particularly SEHRs like Australia's PCEHR. As this study is focused on the usability of managing access to health information from the consumer's perspective, I approached potential general consumers including students and the wider community.

A limitation of the study was that it was only focused on usability from the perspective of patients using the system to manage access to their own information. The usability of the protocols from the HCP perspective is also an important aspect to evaluate in the future. In particular, as discussed in Section 4.4, it is important to evaluate usability measures to ensure HCPs understand what they can and cannot access, and that they do not feel they need to justify too many actions that are valid or that they may be investigated for misuse when they have done nothing wrong. Likewise, future work could include follow-up usability and qualitative studies with more diverse user types such users fitting the role of administrator or HA, or carers who may need to manage information for other patients.

The prototype system used by participants was not connected to a real eHealth system, and used simulated data and example healthcare professionals. This was done to avoid the usability issues of EHR systems impacting the evaluations. As the forms being created for managing access to patient information were new and not present in existing systems, I could focus on ensuring the forms and menus were usable and met the design principles discussed in Section 4.4. Existing systems, such as the PCEHR, that might have such a management interface integrated in the future may have a more complex menu system in place. As such, it is important that implementations of the management interface when connecting to existing systems are designed to be usable and evaluated for usability through studies similar to the one presented in this chapter.

4.5.2 Methods

The study used a standard usability testing methodology using six scenarios for participants to work through while using the "think aloud" protocol (Jaspers et al., 2004). The think aloud protocol involves participants vocalising their thoughts while using the system and is a standard usability testing protocol that helps understand what a participant is thinking while they complete the scenarios, including their reactions and frustrations. The methodology has been employed in a variety of settings, including various studies of the usability of health systems (Shyr et al., 2014; Kushniruk et al., 2005).

The exact number of participants needed for an individual study can vary and the decision should consider the complexity of the system and context of the study (Macefield, 2009). Traditionally, a minimum of five participants is considered sufficient to discover the majority of usability issues in a study (US Department of Health & Human Services, 2015). However, studies have found that with five participants, a minimum of 55% of problems and an average of 85.55% were found. While a study with 20 participants was found to uncover a minimum of 95% of usability problems with an average of 98.4% (Faulkner, 2003). For the first usability study with the IAF, we deemed 20 participants to be sufficient based on previous studies while allowing us to perform a qualitative analysis of participant responses.

To begin the study, participants were first asked some general demographic information with their gender, which age range they fell into, how many times they visited healthcare providers, and whether they had used any healthcare websites/systems such as the PCEHR before. The participants were then asked to use the IAF prototype to complete a set of scenarios that explored the expected activities a patient would take in an Accountable-eHealth system. The scenarios are outlined in Section 4.5.2.1.

The scenarios the participants completed, which are described in detail in Section 4.5.2.1, included: granting a HCP access to their eHealth record, restricting a HCP's access to specific types of information, reviewing a notification of potential misuse of their information, submitting inquiry requests, and reviewing responses to inquiries by the example HCPs. Participants had the task for the given scenario explained, but were not given any detail on how to complete it. Participants were encouraged to "think aloud" while completing the tasks.

The raw data recorded from this study included the screen cast of the participant interacting with the site, and their responses in the interview. The metrics that were recorded for analysis were:

- Time to complete tasks
- Number of errors while completing tasks
- Rate of successful completion of each task
- Subjective measures - Participants interview responses

4.5.2.1 Scenarios

The participants were given instructions for six scenarios that explore the expected activities a patient would undertake in an Accountable eHealth system. The instructions presented to participants did not give any details on how to accomplish the tasks. The completion of these scenarios was recorded via screen capture.

Scenario 1 – Giving consent

The patient needed to consent to the use of their health information by configuring access to one of their healthcare professionals. This involved the following instructions: "Grant access to your dermatologist, Dr. X, to access your health record."

The expected steps involved were:

1. Navigate to the form to manage access to your health information.

2. Navigate to the form to change access for your dermatologist, Dr. X.

3. Grant them access to your health record

Scenario 2 – Restricting access to data

Instruction to participants: "Restrict your dermatologist's (Dr. X's) access to your mental health-related information."

The expected steps involved were:

1. Navigate to the form to manage access to your health information.

2. Navigate to the form to change access for your dermatologist, Dr. X.

3. Restrict their access to your mental health history

Scenario 3 – Restricting access to data conflicting with HA policies

Instructions to participants: "Restrict your dermatologist's (Dr. X's) access to your sexual health-related information."

The expected steps involved were:

1. Navigate to the form to manage access to your health information.

2. Navigate to the form to change access for your dermatologist, Dr. X.

3. Restrict their access to your sexual health history

4. Observe the warning displayed by the system

Scenario 4 – Reviewing a potential misuse case

Instructions to participants: "You receive a notification that a healthcare professional you're seeing accessed your data that may have breached your policy and requires your review, which you can either mark as OK or submit an inquiry request asking them to explain why they breached your policy. Review the access event and submit an inquiry request."

The expected steps involved were:

1. Click one of the entry points for the notification (either in the top-right hand corner or in the main page). This will take you to the log entry

2. Review the log entry and decide whether or not request an inquiry or mark the information use as OK

Scenario 5 – Reviewing an inquiry response (Misuse)

Instructions to participants: "You receive a notification that an inquiry request you submitted has been responded to by the healthcare professional. Review their response and the result from the system."

The expected steps involved were:

1. Click one of the entry points for the notification (either in the top-right hand corner or in the main page). This will take you to the log entry

2. Review the log entry which has been marked as not OK and will be investigated by the Health Authority.

Scenario 6 – Reviewing an inquiry response (OK)

Instructions to participants: "You receive a notification that an inquiry request you submitted has been responded to by the healthcare professional. Review their response and the result from the system, and decide whether to submit it for further review."

The expected steps involved were:

1. Click one of the entry points for the notification (either in the top-right hand corner or in the main page). This will take you to the log entry

2. Review the log entry which has been marked as appropriate by the system, and decide whether this is accurate and if not, submit for further review by the Health Authority

4.5.2.2 Semi-structured interview

Following the use of the system, an audio recorded semi-structured interview was conducted with the participants. The questions posed to each participant after using the system were:

- Would you use such a system for managing access to your health data?

- Did you have privacy concerns as you used it?

- Could you understand the information the system presented?

- How easy or hard was it to manage access to your information in the system?

- Were there any tasks you found difficult?

- Do you have suggestions for improvement?

4.5.3 Recruitment and Participants

Participants were recruited through emails to mailing lists, having contacts forward the invitation, snowball sampling, and through flyers in the local area as needed.

Table 1: Age range of participants

Age range	**Number of participants**	**% participants**
18–30	11	55
31–50	5	25
50+	4	20
Total	20	

Table 2: Gender of participants

Gender	**Number of participants**	**% participants**
Male	11	55
Female	9	45

I endeavoured to have a roughly even number of male and female participants, and aimed to have representation from at least the following age ranges: 18–30, 31–50, and 50+. This helps give a better evaluation of the usability of the system to different demographics.

There were 20 participants in the study. Participants ranged from 21 to 58 years old with a mean of 35 (SD = 12.7), and there was participation from each age group of 18–30, 31–50, and 50+ as seen in Table 1. 11 (55%) were male and 9 (45%) were female as shown in Table 2.

The majority (55%) had used healthcare websites before, including for health information and for managing their health such as the Medicare website. All stated that they went to healthcare providers at least once a year, with 6 stating they visited healthcare providers more than five times a year. None of the participants were users of the PCEHR/MyHR, but some had heard of it.

4.5.4 Results and Analysis

In each scenario except for Scenario 4, participants successfully completed all tasks. Scenario 4 had one participant who did not complete the task due to an error. A summary of the number of errors made by participants and the time taken to complete each task is presented in Table 3.

Table 3: Statistics from the scenarios

Scenario	% completion	Critical errors	Non-crit. errors	Avg. time (mm:ss)	Min. time (mm:ss)	Max. time (mm:ss)
1	100	0	3	00:42	00:10	02:26
2	100	0	4	00:44	00:09	02:15
3	100	0	0	00:26	00:12	01:08
4	95	1	1	00:39	00:09	01:40
5	100	0	0	00:35	00:18	01:11
6	100	0	0	00:29	00:13	00:52

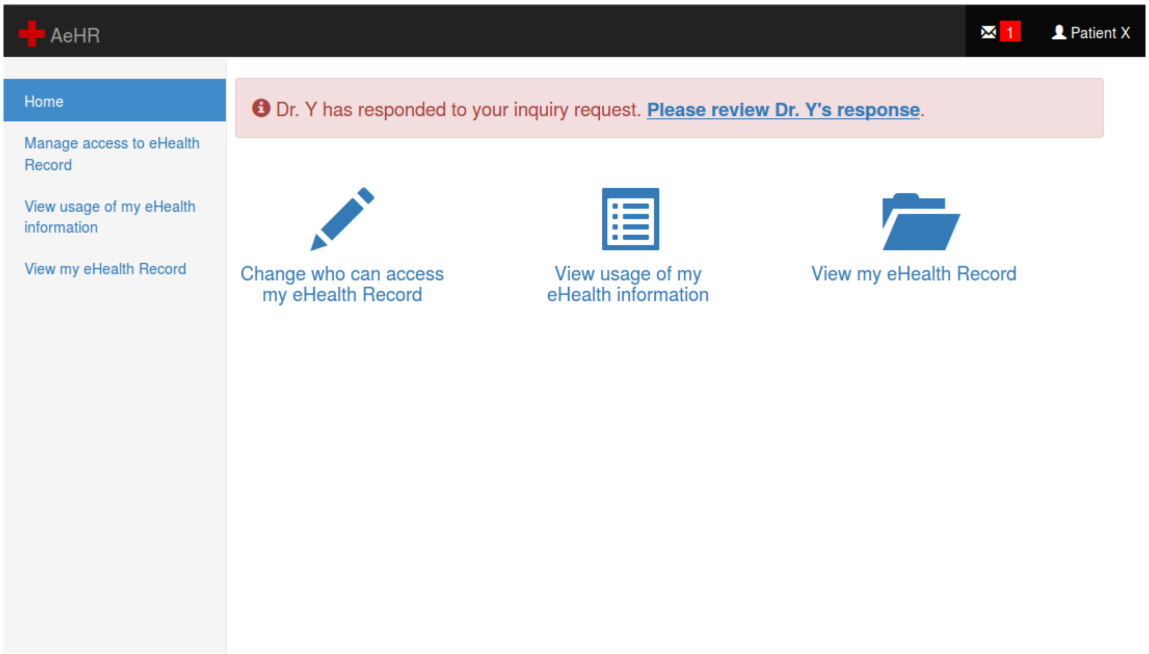
In general, the moderating factors of age and gender did not have a significant impact ($p > 0.05$) on the number of errors encountered or the time taken for each task. There was a slightly significant correlation between age and the time taken to complete Scenario 2 ($r = 0.47$, $p < 0.05$), but the remaining scenarios did not see a significant correlation. This shows that in terms of completing the tasks successfully, the usability of the system was not significantly different for users in different age groups or based on gender.

4.5.4.1 Usability analysis

In analysing the study results, I looked at a number of factors including the completion rate, error-free rate, non-critical errors, and Time on Task (ToT). In addition to this, subjective measures were collected and analysed from comments from participants both during the task as part of thinking aloud, and in response to the semi-structured interview.

Completion rate

The completion rate for a given scenario is the percentage of test participants who complete tasks successfully without any critical errors, and is summarised in Table 3. A critical error refers to any error that results in either an incorrect or an incomplete outcome for the given task. There was one critical error during the scenarios which occurred in Scenario 4. The participant when tasked with submitting an inquiry for



AeHR

✉ 1

Patient X

Home

Manage access to eHealth Record

View usage of my eHealth information

View my eHealth Record

Dr. Y has responded to your inquiry request. Please review Dr. Y's response.

Change who can access my eHealth Record

View usage of my eHealth information

View my eHealth Record

Figure 12: Notification shown when completing Scenario 6

an access event, instead clicked “Mark as OK” and believed the task complete. The participant stated they had forgotten the goal of the task. This was not assessed as a usability issue as the participant did not misunderstand the meanings of the options in the interface.

Errors and error-free rate

The error-free rate is the percentage of participants who complete a given scenario without any critical or non-critical errors. A non-critical error is defined as an error that does not affect the final result of the task, but causes the less efficient completion of the task, such as navigating to the wrong option initially.

Through the use of the think aloud protocol, errors were able to be put in perspective or in some cases disregarded as an error. For example, while normally it would be a non-critical error if on one of the first three scenarios, a participant navigated to the usage logs first, rather than going directly to manage access to their eHealth information, one participant while completing the task said they knew to go to managing access, but wanted to look at the logs first as they would do that before making a decision to restrict access further.

In addition to the one critical error mentioned above, there were eight non-critical errors over the six scenarios. In Scenario 1, two of the three non-critical errors were due to the participants initially selecting “No” on the form to grant access to their health record, before later correcting this to “Yes”. The third error in Scenario 1 was due to a participant first navigating to the option to view usage of their health information, before realising they were in the wrong place and working back to the form to manage their access. They stated this was because they didn’t read the buttons before clicking one. The four non-critical errors in Scenario 2 were due to participants first navigating to the option to view the usage logs of their eHealth information, and in all cases quickly corrected themselves and navigated to the form for managing access to their health information. This was identified from the interviews afterwards as being likely caused by confusion over the wording used in the interface. In Scenario 4, the non-critical error encountered was due to the participant first attempting to navigate to “View my eHealth record” before switching to view the usage of their eHealth information.

Time on Task

Time on Task (ToT) refers to the time to complete a scenario, and is measured from the time the participant begins the scenario to the time they complete the task. A summary of the ToT for each scenario is shown in Table 3. There is a drop in time between Scenarios 2 and 3, even though the tasks are roughly the same, as the participants are then more familiar with the interface for managing access.

Subjective analysis and issues raised by participants

During the completion of tasks, even when errors in actions did not occur, usability issues were identified from the comments from the participants while “thinking aloud”.

During Scenario 1, one participant was concerned with granting access to Dr. S with the participant stating “I probably wouldn’t feel comfortable granting a dermatologist full access to my eHealth record” and “it would be good if there was an option to say, should Dr. S have access to your eHealth record either in full or part or something like that.” As this was the first scenario, they had not yet experienced the options to restrict access to their health record further and determine the information that would be available to the doctor. This was a failure of the interface to make it clear what information would be available to the HCP by default when the participant selects “Yes” to grant initial access to their record, and that they have the option of further restricting access. This was a violation of our usable security design Principle 2 identified in Section 4.4.1. Likewise, per Principle 3, the most secure option, in this case having default restrictions in place, should be made obvious. These comments did, however, provide evidence of the concerns over control of their information that the IAF aims to address.

In Scenario 2, in addition to the four participants who first navigated to the option to view the usage logs of their eHealth information, a further two participants were initially unsure of which option to click and considered clicking the view usage logs option. From discussions with participants in the interview, this was identified as being likely caused by confusion over the wording used in the interface. As such clearer wording of both options is needed. In particular, some participants found the wording “Manage access to my eHealth information” preferable to “Change who can access my eHealth information” as they felt the latter only referred to “who” and not also to “what” could be accessed.

In Scenario 3, the warning that there is a conflict between the patient’s preference and the HA policy caused some confusion as to why that was the case among two of the participants. Per our usable security design Principle 1, it is recommended that the interface should provide a more descriptive and explicit explanation of the reasons for a HA policy requiring a given HCP has access to certain information so that the patient is able to understand. One participant was unsure if the changes had saved due to the warning, and so the interface should make it clearer that the preference was saved and that the warning is informative rather than a save error. Patients were in general positive about this functionality however, with unprompted comments during the scenario such as “It’s good that it notifies you that they’ll probably still need access to it, so it’s not like you’re going ‘well, that’s it’, saying they can still access it if they really need to.”

In addition to the non-critical errors outlined above, while completing Scenario 4, one participant was unsure of some of the wording on the log entry form, however, the remaining participants indicated the log entries were easy to understand.

In Scenario 5 and 6, participants in general gave positive comments, with unprompted statements such as “It explains exactly why which is good” and “That’s cool, easy and straightforward to use.” However, two participants asked for clarification on how the initial decision from the system was made while reviewing the result from the system. The interface could make it clearer that it is an automated decision from the reasoner.

In Scenarios 1, 4, 5, and 6, participants were given notifications that contained a call to action that would take them directly to the correct form. For example, in Scenario 5 and 6, the interface displayed a notification that they had a response to an inquiry that needed review as shown in Figure 12. While this was the most efficient path to complete the tasks, three participants never clicked a notification while a further five did not initially click a notification but did click the notification in later tasks. When asked about why, multiple participants stated they initially thought that notification was a reminder as to what the task was about rather than thinking it was something they could use.

Opinions on the overall usability of the prototype

In the interviews following the completion of the scenarios, all participants stated they felt the prototype was easy to use and were positive about the usability of the system. Those who made non-critical errors such as initially going to the wrong option were still positive about the usability of the prototype, and stated that the uncertainty over which option to click was quickly made clear to them after exploring the interface.

When asked for initial comments from participants, many noted the ease of use of the prototype without being asked specifically about the usability, with anecdotes such as:

- "It was easy enough, it flowed. The instructions were pretty clear. So, I didn't have an issue reading and understanding what I needed to do."
- "Good usability, pretty easy to use, and I like the sense of control that it gives to the user, which is the public basically the customer."
- "It was very simple to use"

When asked whether they would use such a system for managing access to their health information, some participants again highlighted the usability of the system in their responses. Likewise, in the later interview questions specifically about particular aspects of the usability of the system participants were positive. When asked about how understandable the information presented by the system was, such as the log entries, HCP responses, and options available to patients, none of the participants raised any problems and stated that they thought it was easy to understand. In particular, a number of participants highlighted the way the system differentiated the information and options with visual cues, with comments such as:

- "Everything was very clear, and the buttons were very different so you have no chance of clicking the wrong button. Everything was explained very precisely, and it's pretty easy interface."
- "Yeah, I thought that was really easy to use. I think that obviously there's things highlighted, the different colours really helped, so something red and

the eyes instantly go to it, a lot of those buttons were green so the contrast in colours meant that it was quite easy to find and user friendly in that way."

- "I thought it was easy to understand. The layout was setup so it was easy to follow and easy to use. The prompting is good. Importantly it makes it clear whether information you don't want to be seen but it will be seen. It makes it clear, it tells the story, and it allows you to take it further up the chain to health authorities if need be. So, overall I think it's a well presented, easy to use system."
- "It was well laid out and informative and provided the information that I needed quickly."

When asked specifically about how easy or hard it was to manage access to their information and limit access to certain HCPs, participants once again were extremely positive and highlighted the way the system made it clear what was happening. Additionally, some participants in particular highlighted the system limiting initial options as making things easy to use and avoided it being too overwhelming, with anecdotes including:

- "Very easy, the interface was fairly intuitive."
- "Found it very easy to manage the access, and you can't really do anything wrong as the buttons are pretty clear as to what's going to happen."
- "Three options on the initial screen, I think makes it nice and easy. Everything laid out beyond those initial three options was clear and easy to understand and read."
- "I thought that was pretty easy and straightforward. I like that it's sort of restricted to not too many tabs, it's not very overwhelming."
- "I thought it was really easy. It was easy to be able to change access if you changed your mind and decided that you didn't want Dr. S to have access to mental health, it was very easy to go in there and change from yes to no."

When asked about whether any tasks were difficult or confusing, two participants mentioned their initial confusion over which button to click initially in Scenario 2, but stated they felt that once they had clicked the wrong option, it was clear what they had to do, with one participant stating: “I think Scenario 2, I went to the wrong link first to manage the access, but it was pretty easy to see I couldn’t do it there, and went back and found the other one that needed to be done. It was all very user friendly so it was easy enough” Another participant stated they found it a lot more usable than they had expected when going into the task: “I thought it was pretty straightforward. It was easier than I expected actually, I thought it might be a bit tricky. But I found it pretty easy.”

4.5.4.2 Views of participants on the IAF protocols

All participants were positive about using the IAF protocols to manage access to their data, with very positive comments relating to the use of the framework with SEHRs, such as unprompted comments like “I reckon if we could get this up and running it would be fantastic” and “I hope it takes off!”

In their responses to interview questions about whether to use such a system, 13 participants (65%) mentioned having the ability to restrict access to certain types of information as a positive with no negative comments. Though, 30% stated they were unlikely to restrict access further than the default preferences. 15 participants (75%) specifically mentioned the privacy of the system, with 12 of those comments being positive. Two of the remaining three participants’ comments on privacy were determined neutral in that they weren’t more positive about the IAF’s prototype privacy than other secure online systems, with the participants mentioning they would feel the same about the privacy of such a system as other online systems such as banking and private health insurance. The opinion of the last of those three participants was determined to be negative, with their concerns were focused any private information being available over the web due to recent hacks reported in the news, stating: “I don’t know how this information would be stored, what sort of encrypting it would have. You know, there are a few dodgy doctors out there who could sell your information to drug companies and that kind of thing so I don't know how it works." This participant was positive about the logging and restricting access functionality of the accountability mechanisms, however. Another participant also mentioned being unsure of the safety of any information over the web, which shows the greater awareness of web security due to the increasing number of high profile hacks.

Six participants (30%) mentioned unprompted the property of discouraging misuse of patient information as positive of the system, with one of the participants stating they had prior knowledge of inappropriate access of private health information in a hospital.

Participants were positive about the other accountability functionality, with 40% mentioning positively the ability to view all logs, as opposed to just being able to view entries for alerts for policy breaches. The ability to override policies was mentioned in five responses (25%) with all the comments being positive including two unprompted positive comments made while completing the scenarios. However, four participants (20%) raised concerns over knowing how the HA and the system would decide if overriding was appropriate, showing that policy makers and the system must make it clear to the patient why a decision over use of their information was made. 30% of participants positively mentioned the notifications of misuse when discussing whether they would use such an eHealth system, and 35% of participants positively commented on the ability to follow up on an inquiry response if they disagreed with the result from the system. Some relevant anecdotes related to this include:

- "I didn't have any concerns using it, about privacy, in regards to them breaching anything. And I like the fact that you can see everything and what people have seen and if it's been accepted or been misused. I think there is a great level of privacy to it, and I would feel comfortable using it."

- “Yeah, I thought it was brilliant. I could stop people if I don’t want them to do it, and then if I’m notified if they go there, then that’s good.”

- “I like that you can see everything, not just the ones that you don’t allow and then they get access to, but you can see even the ones that you do allow.”

- ”As we saw obviously there’s going to be situations where they need to override that, I think most people are understanding of the fact that whilst you want information to remain sensitive that in some scenarios it’s important that health professionals are in fact aware of that, but they just want some sort of control. At least, just being aware that ‘yes, I would consider this information sensitive’, but at least having that notification that someone has overridden that... also if you’re still not happy with the reasons they gave you, I think having that ability to down the bottom of that screen where it said notify the health authority, I think that there are going to be people who feel as though, ‘no, my confidentiality was breached, they shouldn’t have accessed that information’, so they’re still given another opportunity to say ‘I’m not happy for the reasons given, and I want to take this further, and I want the Health Authority to look into it further.’ ”

- “I think that this does mean that there are things in place to ensure that health professionals are actually accessing the information they need to, and they’re not just overriding information for the sake of overriding it just for interests sake or for general investigation as one of those said. So, I think that they are given enough control.”

Regarding the use of a shared EHR, 8 participants (40%) pointed to the value of being able to have information stored in one place, not having to transfer information between HCPs, and having access to a long continuous history. The moderating factor of age had an impact on this opinion, with the participants in the age groups 30–50 and 50+ made up the majority (5) of these comments, likely due to their longer medical history. While a number of participants in the 18–30 age range stated that at present they didn’t yet have a complex enough medical history to get the full value of a shared record. Comments related to this included:

- “I had a major operation a while back, and you forget details of it and everything like that. And some of it’s quite pertinent to a physio now, so it’s kind of like having that running history as well. And maintaining the accuracy you see, so it helps when you go to the doctor, the more information you can give to medical professionals these days, the better."

- "When we moved to [another state], I had to try and piece back from the specialist dates and years, and when I went and had scans and cortisone injections before going to a doctor and a specialist here so it would have been easier if it was all on here."
- "I've moved from [one state] to [another state], and I had to go to a new doctor and explain why I was taking this and that or whatever, and I had to remember when I started doing something or other and when I took this and when I took that and you know with family history... It would have been so much easier if I could have just given a link and they could have gotten all my notes from my old doctor. It would be fantastic! Instead having to try to remember, when you know, so much is happening."
- "I'll go to doctors in different states sometimes. So, the good part about that is, that I can have access for both doctors and they can see the history of things that I'm working through. So, there's some benefit for me in that scenario of having dual doctors having access to some of that information."

Three participants (15%) raised concerns over government policy and centralising control of the patient information. Two of these participants were positive about the accountability aspects of the IAF, but had concerns over the centralisation of health information and the availability of information of the web. One of the participants had distrust of centralising health information under the control of the government and was concerned about the potential for government policy regarding the data to change. Two stated, however, that were positive about the accountability measures of the framework itself, with one saying that they would make particular use of the ability to view logs in such a scenario. The third of these participants was positive about both the accountability protocols and centralising of health data for improved healthcare, however, they raised a concern over giving authorities centralised control over their health data and that it could only work if privacy legislation was strictly adhered to. Anecdotes from participants related to this include:

- “Anything that’s online, I don’t know what happens to it, I just trust that the powers that be have protections in place. As for having control over the privacy though of what doctors can see, all things considered that’s all safe, no one can just randomly access it or hack into it. That aside, because I have control over what the doctors see, that’s OK.”
- “Centralisation of data like this about peoples’ history, personal history, medical history is a good thing if it’s used within the right legal framework. Within the wrong legal framework or an altered legal framework, such as the PATRIOT Act in America for example, or something that’s really bordering on a police state kind of legislation/framework, then this could be something that people just wake up to and not use. So, I think it comes down to the awareness of people making sure that when this thing is rolled out that people understand that there is a legal framework around this centred on human rights. [...] Speaking personally, I think I would use the system, because I think there is a good legal framework in place at the moment and it’s easy for me to know what all my history is. [...] So, I think overall it’s a positive thing.”

4.5.5 Discussion

Overall, the usability study found that participants were positive towards the use of the IAF. Many participants highlighted the usability when asked if they would use such a system for managing access to their health information, showing the positive impact usability can have on the acceptance of such systems. A number of usability issues in the interface of the prototype were identified and were rated for severity based on their the impact the issue has on the successful completion of a task, and the frequency of the issue, which refers to the percentage of participants who encountered a problem.

Participants were in general positive towards SEHRs and the sharing of their health information in combination with the IAF. A number highlighted the value of being able to have the information in one place, have a continuity of care, and easily transfer information between doctors. This was particularly mentioned by those in the 30+ age ranges, likely due to having developed longer and more complex medical histories than those in the 18–30 group had so far.

There were, however, some concerns around both the security of any information shared over the web, and around distrust of centralised and/or government control of information. This greater awareness of the security and privacy of their information is understandable given the prevalence of breaches of web information in recent times, and it is essential that the IAF is part of an overall strategy for securing health information as described in section 3.4. It is also important that an appropriate government policy is both in place and communicated effectively to consumers. The need for a mandatory breach notification law in Australia has been highlighted previously to ensure consumers are informed if their information is compromised and the recent draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Attorney-General's Department, 2015) is a positive step in this direction.

4.6 Conclusion

In this chapter, I have described the initial prototype implementation of the IAF in a simulated EHR system. This implementation was used to demonstrate and validate the functionality of AeH systems. This prototype is used as a base for the experiments presented in this thesis.

I have discussed the usability of the accountability mechanisms in the IAF. Usability guidelines for the design of AeH systems have been discussed. The analysis of the prototype of the IAF was used to improve the prototype's usability.

In previous work on the acceptance of the IAF protocols, users did not actually experience how the IAF would work in practice, as the IAF was not implemented but simply described while surveying them. Using the improved prototype, a user study using standard usability testing protocols was conducted with participants performing in the patient role in the system. Participants were able to use the prototype and provide feedback on both the IAF protocols and the prototype's usability. From this study, it was verified that the IAF protocols could be implemented in a way that is usable for patients using the usable security principles and recommendations discussed in Section 4.4. It was also found that participants were very positive about the use of the IAF protocols and the usability of the prototype. The feedback and the usability issues identified when analysing their use of the system were used to identify recommendations to improve implementations of the IAF protocols.

In the next chapter, I discuss expanding the IAF protocols to enable delegation of access and the security risks associated with the accountability mechanisms, both of which are used to improve the initial prototype.

5 Extending the IAF Model

The initial IAF model assumed all users have an equal ability to interact with the system. However, there are a number of reasons that someone may require another person to act on their behalf in an eHealth system. For example, parents may need to act on behalf of their children; or a carer or another trusted individual may need to act on behalf a person with a disability. As discussed in Section 3.3 when defining our threat model, it is essential that accounts are not shared in an accountable system and there is a threat of unauthorised access by an insider in such scenarios. For the IAF to meet the needs of these stakeholders while maintaining accountability, it must be expanded to support support more diverse use cases with users being able to grant revocable, time-dependent access for someone to act on their behalf.

Two key components of the IAF are the patient usage policies and provenance log mechanisms. Usage policies provide the rules that the framework uses to determine appropriate use of information, and provenance logs are the key to holding users accountable for their actions in the system. While previous work on the IAF has addressed the use and representation of these mechanisms, the security and privacy implications of these accountability mechanisms themselves must also be considered as discussed in Section 3.3 when defining our threat model. Both usage policies and provenance logs will often themselves contain information that could be considered sensitive. For this reason, these must be properly secured from unauthorised access. Additionally, for provenance logs to serve the purpose of holding someone accountable, it must be possible to prove they have not been tampered with.

In this chapter,[3] I first define the requirements for delegation of access in the IAF and explore its implementation in the prototype for eHealth systems. I then explore the privacy and security issues surrounding usage policies and provenance logs in the IAF. These are essential considerations when implementing the IAF protocols.

[3] Publications related to this chapter: Grunwell and Sahama (2016); Grunwell et al. (2015b)

5.1 Implementing delegated access in the IAF

Delegation of access or delegation of authority involves granting access to a user to be able to acquire the set of permissions of another user in the system. By doing so, they are able to act on that user's behalf (Barka and Sandhu, 2000). In an RBAC system, this can involve granting the roles of one user to a delegate. However, in complex access control situations, determining which permissions should be delegated and restricting those permissions to only specific delegates, rather than all users of a given role, can be difficult. Through usage policies defined in an IAF, we can define policies for delegation of access that allow for specific actions to be performed on another user's behalf while maintaining accountability.

In this section, I define the properties delegated access should have in the IAF, explain why they are required, and describe how they can be implemented.

5.1.1 The need for delegation of access in Accountable-eHealth systems

In an accountable system, it is essential that it is clear who is performing a given action so that they can be held accountable in the event of misuse. Therefore, it follows that it is important that accounts are not shared. However, not all users have the same ability to interact with a system. It is common, for example, for people with disabilities to share access to accounts with carers or family members (Singh et al., 2007). Likewise parents may manage their children's healthcare-related accounts. Therefore, it is necessary to include functionality that enables patients to delegate control over their EHR to a trusted person (Alhaqbani and Fidge, 2007). An AeH system must support these use cases while ensuring the actual person performing the action can be identified and held accountable if necessary. In the previous work developing an initial IAF model, patients were assumed to be a homogeneous group with an equal ability to interact with an eHealth system. The IAF model needs to be expanded to provide for diversity of users, including enabling users to grant

```
<o:policy xmlns:o="http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov
   " type="http://w3.org/ns/odrl/2/privacy" uid="policy-use-ehr">
  <o:permission>
    <o:asset uid="urn:ehrUsagePolicy:12318" relation="o:target"/>
    <o:party uid="urn:healthAuthority:1458" role="o:assigner"/>
    <o:party uid="urn:healthProfessional:10946" role="o:assignee"/>
    <o:action name="o:modify"/>
    <o:constraint name="o:dateTime" operator="o:lteq"
      rightOperand="2015-06-10"/>
  </o:permission>
</o:policy>
```

Listing 3: Time-dependent policy

permission for someone to act on their behalf.

While patients delegating control over their EHR policies is anticipated as the primary use case for delegated access, there may also be reasons under certain conditions where a HCP may delegate access to others for limited purposes such as in order to have an assistant add information to a patient's record. Such situations can be limited by policies set by the HA to control what delegated access can be granted in what context.

5.1.2 Requirements for delegated access policies

In order to implement delegated access in the IAF, we considered the use cases of the intended users of the system and previous work in the area. As discussed in Section 3.3, the main threat we are addressing through providing delegated access is to discourage and reduce the need for account sharing. Account sharing is common in cases such as people with certain disabilities sharing access with carers (Singh et al., 2007; Alhaqbani and Fidge, 2007) and parents may need to manage their child's record. In both of these cases, the access can be time-limited, so it is necessary that delegated access policies can expire. Likewise, a given carer may not need total access to a record, or a doctor's assistant may not need all the access to a patient's information that the doctor has in order to perform their duties, therefore, the policies should be granular and allow limiting access to certain information or actions. Additionally, it is important that the user delegating access to certain health information is not only able to grant, but also efficiently revoke access when needed (Li et al., 2013).

A summary of the requirements I have identified for the usage policies set by the user delegating access when implemented in the IAF are as follows.

Easily revocable

Policies for delegation of access must be easy to revoke. If the data owner or other user with the authority to grant access to an EHR decides the user who has been granted delegated access should not be able to perform the granted actions any more, then the process to revoke the policy should be simple and take effect immediately.

Time-dependent

These policies must be able to be limited to a specified period of time. This is important so that a policy will expire when a person's need to have someone act on their behalf is gone. Examples of when this would be needed include:

- A parent's access to manage their child's EHR should expire when the child turns 18

- A carer with a limited term employment with a particular patient should have their access expire on their contract conclusion date

Granularity

These policies must be as granular as the usage policies set on HCPs by patients. Rather than just being able to grant complete access to act on someone else's behalf, the policies should enable users to grant access to specific actions and/or types of data in limited contexts and prevent access to everything else. Likewise, the HA must be able to limit how much access can be granted to different users depending on the context. Examples of granular policies include:

- A nurse in a General Practice may need to perform actions on non-sensitive information for a patient record that a doctor in the practice has been granted access to. For example, the nurse may update certain patient details or add non-sensitive information, but they should not have access to anything else in the record

- An assistant may need access to add information en masse without needing to see existing record entries, and so can be restricted to be only able to append items to the record and only view items they added

Policy included in provenance log

As with the usage policies set by patients on their HCPs in the existing IAF model, the policy used to perform an action on behalf of another user must be captured in the provenance log entry.

5.1.3 Representation

As discussed in Section 4.1.2, it is important to have a way to represent and manipulate the policies in the IAF system, in particular for interoperability. ODRL can be used to represent access delegation policies and meet the requirements of such policies. The restrictions placed on the access policy including who the access is delegated to, the expiration of the access, and the types of actions, data and the contexts for which the access is granted can all be expressed in ODRL through *constraints* and *duties*.

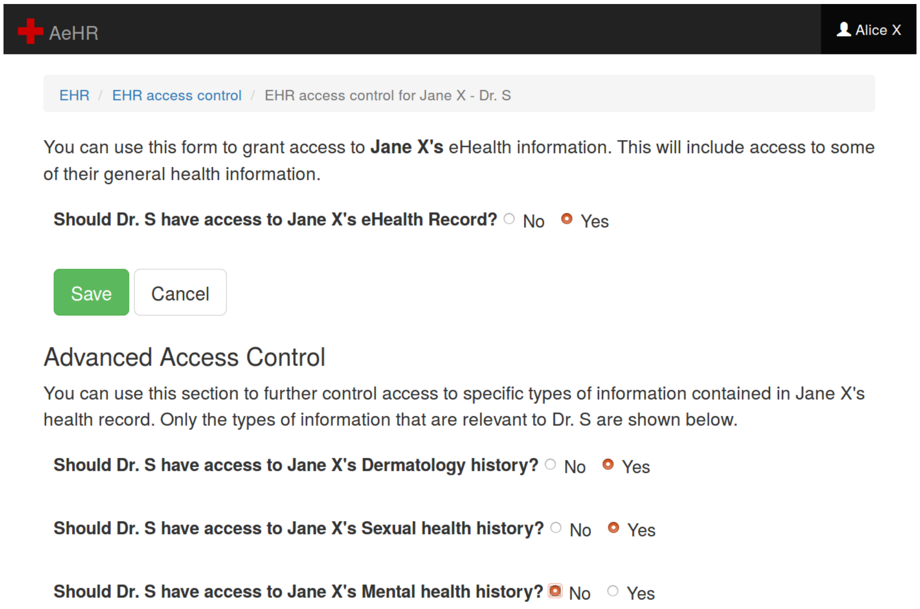
Time limits can be defined in “dateTime” constraints. As an example, Listing 3 shows a policy represented in ODRL where a member of a Health Authority has granted access to a carer to modify a patient’s usage policies for their EHR. In this

```
<o:policy xmlns:o="http://odrlextension.org/ns/odrlx/2x" xmlns:eh="
    urn:ehealth.gov" type="http://odrlextension.org/ns/odrlx/2x/
    privacy" uid="policy-use-ehr">
  <o:permission>
    <o:asset uid="urn:ehrUsagePolicy:12318" relation="o:target"/>
    <o:party uid="urn:healthAuthority:1458" role="o:assigner"/>
    <o:party uid="urn:healthProfessional:10946" role="o:assignee"/>
    <o:action name="o:modify"/>
    <o:constraint name="o:dateTime" operator="o:lteq"
      rightOperand="2015-06-10"/>
  </o:permission>
  <o:transaction uid="transaction-modify-policy" valid="o:true" type=
      "o:policyManagement" dateTime="o:20140601112233" location="urn:
      emrlocation.org/10946">
    <o:asset uid="urn:ehrUsagePolicy:12318" relation="o:target"/>
    <o:party uid="urn:healthProfessional:10946" role="o:user"/>
    <o:action name="o:ehrUsagePolicy/Modify"/>
  </o:transaction>
</o:policy>
```

Listing 4: Transaction log of a delegated access event

policy representation, a permission is granted for the asset “ehrUsagePolicy:12318” which refers to the usage policy for the patient with ID 12318. This policy has been created by the HA represented by the “assigner” entry for “healthAuthority:1458” and the permission is assigned or granted to the HCP with an ID of “healthProfessional:10946”. The permission granted is represented by the “action” which allows modifying the usage policy. The constraint limits the validity of this policy so that it expires on the 10th of June 2015 by defining a “dateTime” constraint that is less than or equal to that date.

When an action is logged, it is important the current state of the policy used to determine if the action was compliant needs to be captured. We can represent transaction logs in ODRL with the current policy included in the log. Listing 4 shows a transaction log of a carer modifying the usage policy of a patient which includes the policy from Listing 3 as well as the event context for a modification of the usage policy for the patient by the carer.


AeHR
Alice X
EHR / EHR access control / EHR access control for Jane X - Dr. S
Save
Cancel

You can use this form to grant access to **Jane X's** eHealth information. This will include access to some of their general health information.

Should Dr. S have access to Jane X's eHealth Record? ○ No ● Yes

Advanced Access Control

You can use this section to further control access to specific types of information contained in Jane X's health record. Only the types of information that are relevant to Dr. S are shown below.

Should Dr. S have access to Jane X's Dermatology history? ○ No ● Yes

Should Dr. S have access to Jane X's Sexual health history? ○ No ● Yes

Should Dr. S have access to Jane X's Mental health history? ● No ○ Yes

Figure 13: Alice X managing Jane X's usage policies

5.1.4 Verification

The initial prototype developed in Chapter 4 was extended to include the devised access delegation requirements. A number of expected scenarios were developed to demonstrate and verify the functionality of the delegated access in the prototype AeH system. Additionally, the requirements for delegated access in the IAF were modelled using UPPAAL. In this section, I detail theses scenarios and the developed model.

5.1.4.1 Case scenarios

In this section, I describe three scenarios that demonstrate different hypothetical situations and outcomes. These scenarios demonstrate the necessity for delegated access, and are used to test and validate the functionality of the implemented requirements for delegated access in the IAF in prototype systems.

Scenario 1

In Scenario 1, a parent is given complete access to manage their child's EHR, including granting HCPs access to the record, modifying their usage policy, and reviewing log entries. The policy will be set by the managing health authority and will be set to expire on the date of the child's 18th birthday or another date relevant to the given legal system.

In the scenario, the parent, Alice X, is taking their child, Jane X, to a new dermatologist, Dr. S. Alice X grants Dr. S access to their child's record, but restrict access to the child's mental health history. During an investigation, deeming it necessary to provide appropriate care, Dr. S overrides the usage policy to access Alice X's mental health history. Jane X is notified of this and submits an inquiry asking Dr. S to explain his actions. Figure 13 shows the view of Alice X managing Jane X's usage policy in the example AeH system.

Scenario 2

In Scenario 2, a healthcare worker, Bob, is given access to manage the record of a patient with a mental disability under their care. The access is granted by the relevant health authority and is set to expire at regular intervals requiring explicit renewing of the policy subject to review.

An example flow in this scenario is that Bob grants access to view the patient's record to a General Practitioner, Dr. Y, who the patient is seeing for a chest infection. The GP by default does not need access to the patient's mental health history, but during the treatment, needs to prescribe a medication that may have side effects when combined with other medication. As a result, Dr. Y queries current medications the patient is taking, which includes parts of the mental health record. This is flagged for review in the patient's log, but, understanding the situation, Bob marks the access event as OK.

Scenario 3

In Scenario 3, a doctor grants access to one of the nurses caring for one of his patients to add data to the record. The access is granted by the doctor and will be revoked upon the patient's discharge from the hospital. The access is limited so that

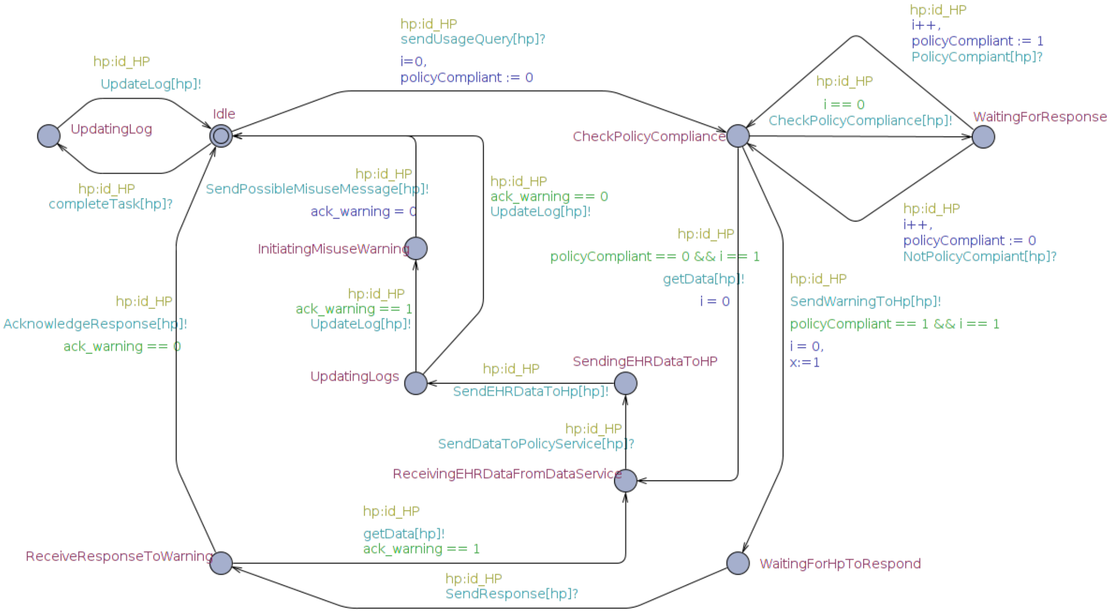


Figure 14: Usage Query Service model in UPPAAL

the nurse can only view the items that they added in the record. This is represented in the policy as an extra constraint on whether the nurse is the author of the item being viewed. The nurse adds three items to the record, and can view them in the interface in order to review and correct them. Upon attempting to view an unrelated area of the patient's record, they are denied access.

5.1.4.2 Modelling access requirements

The requirements for delegated access in the IAF were modelled using UPPAAL, using the initial IAF model developed previously by Gajanayake (2013) as a starting point. UPPAAL is a model-checker jointly developed by Uppsala University in Sweden and Aalborg University in Denmark that enables the verification of real-time systems that can be modelled as networks of timed automata (Behrmann et al., 2004). Its main components are a system editor for creating models, the *simulator* that allows you to simulate the behaviour of the system, and the *verifier* which analyses the model's behaviour.

In an UPPAAL model, a system is expressed using a graphical notation with

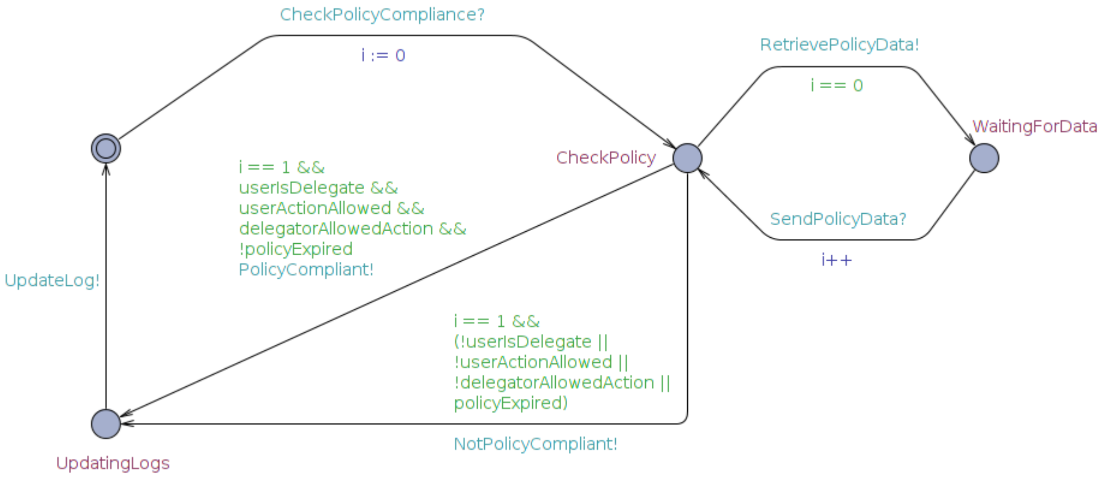


Figure 15: Delegated Access Usage Query model in UPPAAL

variables, clocks, and synchronisation channels. There are two types of synchronisation channels which are used to synchronise two automata in the system: an input channel represented as a variable name followed by a `?` (i.e. `Variable?`), and an output channel represented as a variable name followed by a `!` (i.e. `Variable!`). When a output channel is invoked in the system, the corresponding input channel is triggered allowing communication between the automata.

In order to analyse the behaviour of the modelled system, the verifier allows checking specific characteristics of the system through the user of queries. When running a query, UPPAAL uses a "brute force" approach to exhaustively check all paths through the model to verify if the specific property of the system that is being query holds.

UPPAAL version 4.1.19 was used for this simulation. Figure 14 shows the initial IAF model's usage query service modelled in UPPAAL. When looking at delegation of access, part of the "CheckPolicyCompliance" step of the usage query service, shown in the top right section of Figure 14, was modelled.

The access requirements for delegation of access in the IAF were modelled using UPPAAL. Figures 15 and 16 show the IAF's usage query service steps for checking

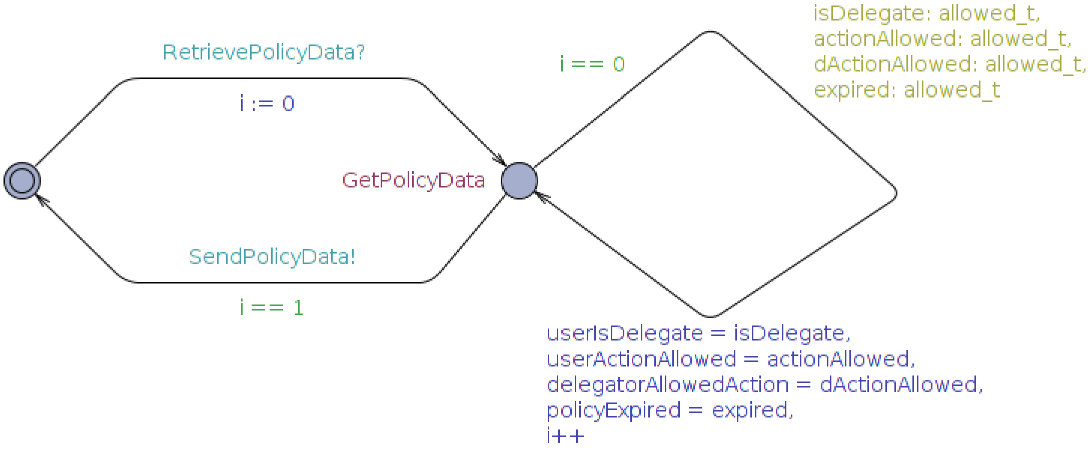

RetrievePolicyData?
i := 0
i == 0
isDelegate: allowed_t,
actionAllowed: allowed_t,
dActionAllowed: allowed_t,
expired: allowed_t
GetPolicyData
SendPolicyData!
i == 1
userIsDelegate = isDelegate,
userActionAllowed = actionAllowed,
delegatorAllowedAction = dActionAllowed,
policyExpired = expired,
i++

Figure 16: Policy Data model in UPPAAL

delegated access modelled in UPPAAL. We define a user "Bob" who will act as the user who is delegated access for a given action. Using the *verifier* on this model, we can test the defined requirements for delegated access are satisfied. We do this by checking whether there is a path through the tree of reachable states in the model that to a given state. For example, to check that there exists a path where access is allowed to modify a patient's usage policy by a delegate we can use the following query:

```
E<> (userIsDelegate && userActionAllowed && !policyExpired && Bob.
    ModifyUsagePolicyForPatient)
```

The result from the *verifier* for this query is "Property is satisfied", meaning our requirement is met. Then we can verify that there does not exist a path that would grant access to modify the policy when the delegate policy expires or if the user is not a delegate using the following queries:

```
E<> (!userIsDelegate && Bob.ModifyUsagePolicyForPatient)
```

```
E<> (userIsDelegate && policyExpired && Bob.
    ModifyUsagePolicyForPatient)
```

Both of these queries result in “Property is not satisfied”, verifying that there is no such path in the model and our requirement is met. Additionally, it is important that a user cannot delegate access to perform an action they themselves cannot perform. To verify there does not exist a path where Bob can perform an action that the user who delegated access to Bob cannot perform, we can use the following query:

```
E<> (userIsDelegate && userActionAllowed && !delegatorAllowedAction
    && Bob.ModifyUsagePolicyForPatient)
```

Using this method to test the model, I was able to verify that the protocol met the delegation of access requirements defined in this chapter.

5.1.4.3 Implementation

As part of validating the IAF protocols, I explored implementing them into existing EHR systems. This was done using the open source OpenEMR, which is used around the world, and FluxMED, a customisable EHR system designed to easily collect and manage different types of medical data. In Chapter 6, I demonstrate the implementation of the IAF protocols including the implementation of the delegation of access requirements in OpenEMR in Section 6.2.

5.2 Security and privacy requirements for policies and logs

Two key components of the IAF are the patient usage policies and provenance log mechanisms. Usage policies provide the rules that the framework uses to determine appropriate use of information, and provenance logs are the key to holding users accountable for their actions in the system. The unauthorised viewing or modification of usage policies, purposes, or provenance logs is a concern due to the information they can contain about a patient’s medical history.

Usage policies defined by patients and the HA are used to determine appropriate

Table 4: Usage policy and provenance log information

Information type	**Usage Policy**	**Provenance log**
Patient identifier	X	X
HCPs patient has sought treatment from	X	X
Health area of HCPs	X	X
Health area of data accessed	-	X
Time of information access	-	X
Location of information access	-	X
Purpose of information access	-	X

use of information in the IAF. They can contain information such as what types of medical treatment the patient which could itself be damaging if leaked.

As discussed in Section 2.6, a key component of an accountable system such as one implementing the IAF are policy-aware transaction logs. In the IAF model and the developed prototype, the framework logs all information access by HCPs, and these logs are made available to patients in a user-friendly format which they can review at any time. The information contained in the log entries includes which HCP accessed the information, the date and time of the event, the purpose or context of the information (i.e. patient visit, consultation, etc.), and whether the access to that information was policy-compliant. Similar to the usage policies, this information if disclosed, could prove damaging to a patient.

In this section, I discuss the information available in the usage policies and provenance logs, risks associated with this information, valid access to this information, and issues and challenges of securing them.

5.2.1 Information contained in usage policies and audit logs

Table 4 lists the information available in the usage policies and audit logs. As provenance logs capture the current state of the usage policy at the time of the event, they contain all the information contained in the usage policy in addition to details of the event.

As mentioned in Section 2.1.1, a patient's health record contains sensitive information, the disclosure of which can cause significant repercussions to the patient (Appari and Johnson, 2010). Patients may consider some of their health information to be more sensitive such as their mental health history or sexual health history. The information in the usage policies may reveal some details about such sensitive information, which could be damaging to a patient if made public. If disclosed they can reveal which HCPs the patient sees for treatment, the types of treatment the patient is currently receiving or has received in the past, and the types of data available in the patient's health record. Revealing that a patient is seeking treatment from a mental health specialist, for example, may be a significant concern for some patients and in some situations could potentially cause socioeconomic issues for them.

The main risks associated with the usage policies and provenance log information in the IAF involve unauthorised access to the information they contain, unauthorised modification of usage policies, tampering with provenance logs, and the possibility of information users to deny they performed an action in the system after-the-fact.

Weak authentication on the part of a patient or HCP (i.e. weak/leaked password, leaving a logged in session unattended, etc.) could lead to the unauthorised access to some of the information they contain. This is why strong authentication mechanisms and training of users is essential, but is currently out of the scope of this work.

5.2.2 Valid access to usage policies

Within an AeH system, a patient's usage policies can only be viewed or modified by a limited number of users, and only in specific situations. Breaking up users into patients, HCPs, and the HA, the following defines what constitutes valid access to usage policies:

- **Patient**: The patient should always be able to view and modify their usage policies. They can change their usage preferences in these usage policies at any time.

- **Healthcare professional**: The HCP should not be able to modify or view patient usage policies directly. They will, however, be informed of their access level to the information they request in a patient's record.

- **Health Authority**: The HA will need to be able to view the usage policies of a patient for the purposes of investigating potential misuse detected by the system. They will also need to be able to verify the integrity of the usage policies and the history of who has modified them. The HA will not be able to modify an individual's usage policy, but can set default policies that may override a patient choice to ensure all necessary information is available to the relevant HCP in order to provide adequate care.

5.2.3 Valid access to provenance logs

In a similar manner to a patient's usage policies, access to view provenance log entries for a patient's health record is restricted depending on the type of user and their relation to the log entry. Once again in terms of patients, HCPs, and the HA, the following defines what constitutes valid access to provenance logs:

- **Patient**: The patient should always be able to access the log entries for their health record. They can review these logs at any time, and submit inquiries for events identified as potential misuse.

- **Healthcare professional**: The HCP should be able to access specific log entries for their patients regarding their own access to that patient's data. The specific entries should be viewable to them when they receive an inquiry requesting that they justify why they needed to access the relevant information in the given situation.

- **Health Authority**: The HA will need to be able to access the logs of any patient for the purposes of investigating potential misuse detected by the system. They will also need to be able to verify the integrity of the log entries and usage policies.

It is important that no user is able to modify the existing contents of the log entries under any circumstances.

5.2.4 Non-repudiation

Due to the central role provenance logs play in accountable systems, it is crucial that they are correct and not alterable (Snodgrass et al., 2004). In such systems, it must be possible to detect if the logs have been tampered with in order to provide non-repudiable evidence of all actions (Haeberlen et al., 2007). Additionally, as previously noted in Section 5.2.1, the provenance information in these logs can itself contain sensitive information that must be protected (Davidson et al., 2011).

In a similar way, usage policies must only be alterable by the patient or an approved delegate, and it must be possible to prove the policies have not been tampered with. Tampering with a usage policy could result in unauthorised access to a patient record that would be seen as valid by the system and would be included in the provenance logs. Appropriate methods of securing and ensuring the integrity of these usage policies in addition to the provenance logs is an essential part of designing AeH systems.

5.2.5 Securing usage policies and provenance logs

There has been a lot of research in the area of preventing tampering of audit logs through cryptographic methods (Holt, 2006; Snodgrass et al., 2004; Haeberlen et al., 2007). A key requirement of tamper-proof logging methods is ensuring the forward security of the logs, that is even if an attacker gains control of the system, all logs captured prior to the compromise cannot be tampered with and so any attempt to modify or remove them can be detected (Yavuz et al., 2012b; Sinha et al., 2014). It is also important that the selected method is append only, and the system can detect deletion of log data.

Secure logging mechanisms often use either symmetric primitives or Public Key Cryptography (PKC) schemes. One way of ensuring the integrity of log entries with forward security is through the use of hash chains, where a different key is generated for each log entry to generate a hash-based message authentication code (HMAC) that is used to verify the integrity of the entry (Sinha et al., 2014). Yavuz et al. (2012a) devised a digital signature scheme called Blind-Aggregate-Forward (BAF) which can efficiently create publicly verifiable, forward-secure signatures to verify the integrity of audit logs. Likewise, the Log Forward-secure and Append-only Signature (LogFAS) logging scheme enables more efficient verification of logs as compared to other PKC-based mechanisms which are often computationally expensive (Yavuz et al., 2012b).

Similar techniques can be used to ensure the integrity of patient usage policies with forward security for each modification of the policy by the patient. Each modification of a patient usage policy should also produce a log entry of the event.

It is also important to implement appropriate backup procedures of logs and policies to prevent corruption and further ensure their integrity. These backups must be treated with the same concern for privacy and security as the main storage of the logs and policies with the appropriate mechanisms in pace to protect them (Ko et al., 2011).

5.2.6 Related work on provenance logs in health

International standards for the interoperability of health systems have been developed including HL7, ISO 27799, CEN 13606 health information, and ISO/HL7 10781.

Health Level 7 (HL7) (HL7 International, 2014a) is a set of ANSI-accredited standards developed to enable interoperability to support the exchange of health-related information across heterogeneous systems. The newer HL7 Fast Healthcare Interoperability Resources (FHIR) standards framework includes specifications for Provenance resources that describe how the retrieved version of a resource came to be in its current state (HL7 International, 2014b). Additionally, overlapping information from these provenance resources are included in the Security Event resources which act as audit logs (HL7 International, 2014c).

The IAF model provides additional information in the provenance logs than in the HL7 specification, including capturing the state of the usage policy at the time of the event. Rather than just providing audit logs, the IAF uses these logs to actively notify data owners of potential breaches and provides consumers with a user-friendly way to interact with these logs. While the HL7 Provenance Resource does include an integrity signature that can be used for limited non-repudiation, this is focused on the integrity of a resource received when exchanging information but does not ensure that stored logs and policies are not tampered with. Additionally, the security and privacy implications of these logs are not explored. This work on security and privacy requirements for provenance logs could be applied when implementing the specifications of the HL7 Provenance and Security Event resources in a system.

5.2.7 Prototype Implementation and Modelling

Access to provenance log entries and usage policies as defined in Section 5.2.2 and Section 5.2.3 was implemented in the IAF prototype described in Chapter 4 for verification as part of the AeH system.

The requirements for access to log entries were implemented in the framework prototype. The service first checks the user for their current role (patient, HCP, HA representative, etc.), allowing the HA access to any log entry in order to fulfil their

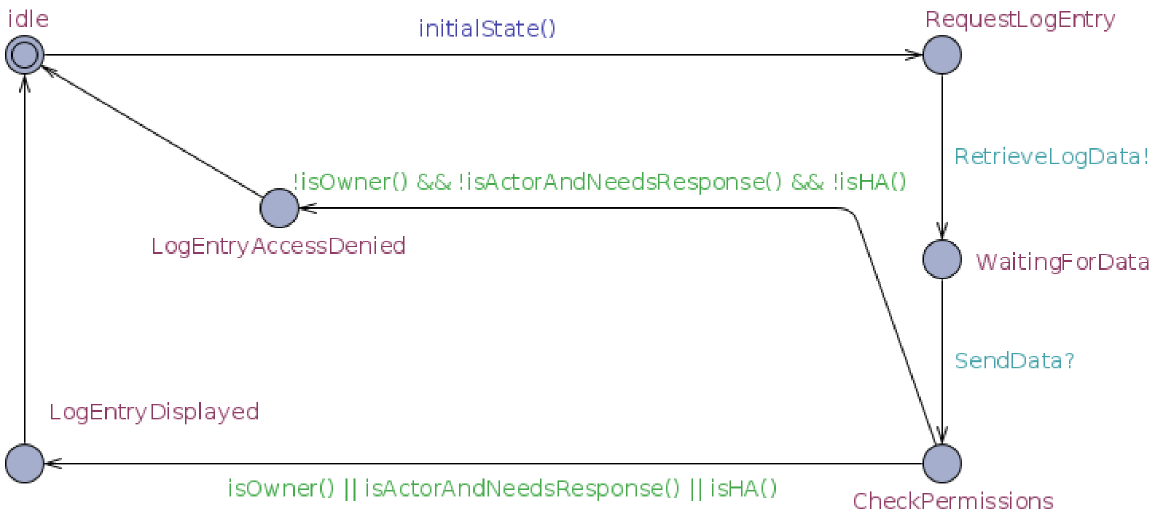


Figure 17: Provenance Log Access Control model

role. Then, if the user is not the HA, the user requesting the data is checked for their relation to the log entry using the entry's metadata, checking whether they are the owner of the log entry (i.e. the patient whose health record was accessed to create the log event), or in the case of HCPs if they were the "actor" who took the action the log entry captures and whether they are required to justify the action taken.

Likewise, the implementation of the access restriction on usage policies was also added to the system. The service takes the current user, metadata about the usage policy, and the action attempted on the policy (read or write) to determine if the current user should be allowed to perform the given action on the usage policy. The owner of the policy will be allowed to both read and modify it, while the HA will only be allowed to read it. No other user is permitted to view the policy.

In addition to implementing the access requirements in the prototype, the algorithms devised were modelled in the IAF protocol using UPPAAL as described in Section 5.1.4.2.

A simple model of the algorithm for accessing provenance logs is depicted in Figures 17 and 18. Using the *verifier* on this model, we are able to test the defined access requirements are satisfied. For example, in order to test that a user is able to

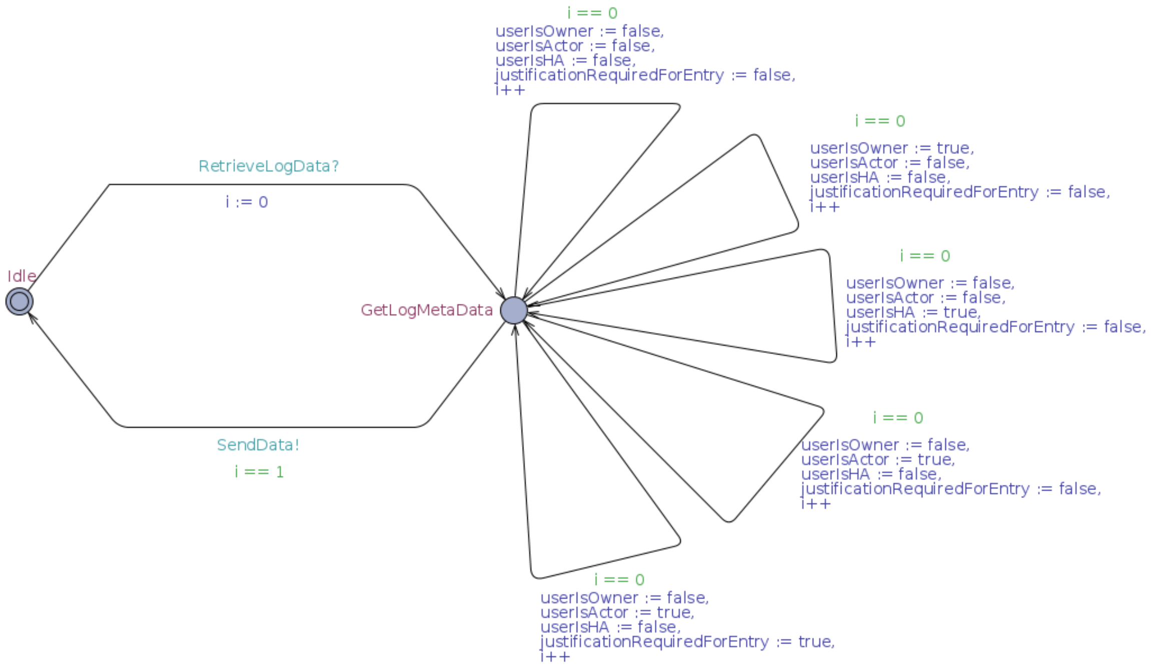


Figure 18: Log data automata model

view a log entry for their health record we can use the following query:

```
E<> (userIsOwner &&
    LogAccessControl.LogEntryDisplayed)
```

This query tests if there is a path where the log entry is displayed to the owner of the log entry. The result from the *verifier* is "Property is satisfied", meaning our requirement is met. To test the requirement that only the owner, HA, or the HCP who performed action can view the log entry, we first verify that there is a path in the model where a user who is not related to the log entry can receive an access denied result using the following query:

```
E<> (!userIsOwner &&
  !userIsHA && !userIsActor &&
  LogAccessControl.LogEntryAccessDenied)
```

This results in "Property is satisfied", which was the desired outcome. Then to verify that there isn't a path that would allow a user who is not related to the log entry to view it, we use this query:

```
E<> (!userIsOwner &&
  !userIsHA && !userIsActor &&
  LogAccessControl.LogEntryDisplayed)
```

This query results in "Property is not satisfied", verifying that there is no such path in the model and our requirement is met.

Using this method to test the model, I was able to verify that the protocol met the access control requirements for the provenance logs and usage policies.

5.3 Conclusion

In this chapter, I defined the requirements for delegation of access in the IAF and explored its implementation in the prototype for eHealth systems. I then explored and discussed the privacy and security issues surrounding usage policies and provenance logs in the IAF, which are an essential consideration when implementing the IAF protocols. Implementing these requirements into both the IAF prototype and when working to implement the protocols in existing eHealth systems, will allow us to design more secure and useful AeH systems.

As part of validating the IAF protocols, I explored implementing them into existing EHR systems which is described in Chapter 6. In doing so, I demonstrate the implementation of the IAF protocols including the implementation of the delegation of access requirements discussed in this chapter in OpenEMR in Section 6.2.

The user study performed in Chapter 4 was performed using the initial prototype which did not include support for delegated access. As part of further evaluating the IAF, we can perform more user studies in the future with more diverse users, including people who may need to manage another person's health record, and HCPs in different roles who may need to have delegated access to perform actions on behalf of another HCP.

In the next chapter, I take the next step from the prototype implementation and demonstrate and discuss implementing the IAF protocols into two existing EHR systems.

6 Implementing the IAF protocols into existing eHealth systems

In this chapter,[4] I implemented the extended IAF protocols into two existing EHR systems, OpenEMR and FluxMED, as two separate case studies. An additional pilot study on the views of healthcare professionals was conducted using FluxMED.

While I have investigated the implementation of the IAF protocols as described in Chapter 4, it is important to determine whether the protocols can be retrofitted into existing EHR systems and how such implementations can be accomplished. In line with a standard approach to research the design of information systems, following the design and development of the prototype discussed in Chapter 4, the next step is to demonstrate the use of the protocols in one or more real-world systems (Peffers et al., 2007). The implementation of the IAF in real-world systems allows the identification of how to implement the protocols and provides a demonstration of how they might work in practice in existing systems. As such, I identified two existing EHR systems to apply the IAF protocols to in case studies. The implementation of the protocols into two different systems provided concrete examples of modifying existing EHRs to include the IAF protocols, and allowed me to investigate how far the unmodified EHR systems are from providing suitable accountability measures.

When implementing the IAF protocols into an EHR system such as OpenEMR or FluxMED, either natively or as a service, it is required that the eHealth data is structured so that the type of data being accessed can be matched with usage policies. Additionally, the EHR system must be modified to log all events with the context of the event and policy used to permit or restrict access to the information, while ensuring the non-repudiation of the log entries. It must also be possible for HCPs to override patient usage policies when the need arises while the system provides

[4] Publications related to this chapter: Grunwell and Sahama (2016); Grunwell et al. (2015a); Batista et al. (2015)

clear communication to the HCP that their action is being recorded and may be investigated if misuse is suspected. This will often require appropriate changes to the front-end of the EHR system as I demonstrate in OpenEMR and FluxMED.

These developed implementations also provide the groundwork for future work on implementing the IAF protocols and AeH systems.

6.1 Existing EHR systems considered

In order to explore implementing the IAF protocols into existing EHR systems, I needed to choose the EHR systems I would use. In this section, I briefly describe the EHR systems considered and why OpenEMR and FluxMED were the EHR systems chosen for the exploration.

When considering which EHR systems to implement the IAF protocols into, a number of open source EHR systems were evaluated due to the availability of these systems for testing. These included OpenEMR (OpenEMR, 2015), FluxMED (Faria-Campos et al., 2014), OpenMRS (OpenMRS Inc., 2015a), and HospitalRun (CURE International, 2015). They were compared against key selection criteria, which are how widely used the system is in similar markets, how data is represented and what types of data can be used, the current access control method and whether there is a role for patients in the system, granularity of access to information, and what existing accountability and audit measures the system employs.

6.1.1 HospitalRun

HospitalRun is a newer system, and while it was the best of the systems investigated in terms of usability, it was deemed not yet suitable due to current limitations in a number of areas at the time of evaluation and not having wide usage at this time. The system is aimed at use in developing world hospitals (CURE International, 2015).

HospitalRun did not enforce types on the information entered at the time of evaluation, though it did allow type-ahead completion for ICD-10 codes for medical conditions at the time. There is a plan to allow the importing of type databases such as ICD-10 in the future (CURE International, 2016). The system employs Role-Based Access Control and does not have a role for patients in the system.

6.1.2 OpenMRS

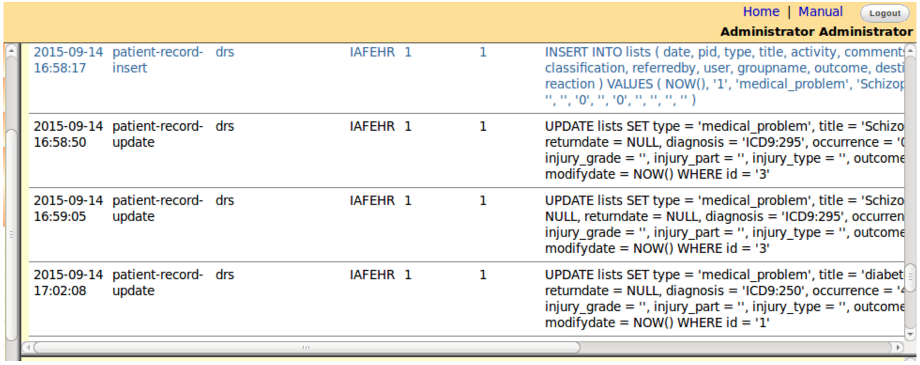
OpenMRS, the Open Medical Record System, is used in various countries throughout the world, but particularly in developing nations (OpenMRS Inc., 2015b).

OpenMRS allows types of information to be optionally mapped to coding standards such as ICD-9 codes for medical conditions or SNOWMED Clinical Terms via imported concepts, which allow us to know the type of information in each entry. OpenMRS makes use of RBAC as its access control method (OpenMRS Inc., 2011), however, it does not currently have the ability to restrict access per patient so that a given physician can only access Patient X's record, but not Patient Y's. Through the installation of a module, it is possible to give patients a role in the system and access to their own records (OpenMRS Inc., 2015c).

OpenMRS does implement some auditing features and has modules that can be installed to keep a trail of changes to data. A since abandoned Access Logging Module was previously found to be inadequate in providing auditing of all user actions in the system in a non-repudiable way (King et al., 2012).

6.1.3 OpenEMR

OpenEMR is an open source EHR system used by many practices throughout the world. OpenEMR allows providing the types of information using imported tables of types such as ICD-9. This is not enforced by the interface however, which is important for being able to define rules based on the type of the data. OpenEMR makes use of RBAC as its access control model (OpenEMR Project Wiki, 2013), but



```
2015-09-14  patient-record-  drs          IAFEHR  1        1          INSERT INTO lists ( date, pid, type, title, activity, comment
16:58:17    insert                                                    classification, referredby, user, groupname, outcome, desti
                                                                      reaction ) VALUES ( NOW(), '1', 'medical_problem', 'Schizop
                                                                      '', '', '0', '', '0', '', '', '', '' )
2015-09-14  patient-record-  drs          IAFEHR  1        1          UPDATE lists SET type = 'medical_problem', title = 'Schizo
16:58:50    update                                                    returndate = NULL, diagnosis = 'ICD9:295', occurrence = '
                                                                      injury_grade = '', injury_part = '', injury_type = '', outcome
                                                                      modifydate = NOW() WHERE id = '3'
2015-09-14  patient-record-  drs          IAFEHR  1        1          UPDATE lists SET type = 'medical_problem', title = 'Schizo
16:59:05    update                                                    NULL, returndate = NULL, diagnosis = 'ICD9:295', occurren
                                                                      injury_grade = '', injury_part = '', injury_type = '', outcome
                                                                      modifydate = NOW() WHERE id = '3'
2015-09-14  patient-record-  drs          IAFEHR  1        1          UPDATE lists SET type = 'medical_problem', title = 'diabet
17:02:08    update                                                    returndate = NULL, diagnosis = 'ICD9:250', occurrence = '
                                                                      injury_grade = '', injury_part = '', injury_type = '', outcome
                                                                      modifydate = NOW() WHERE id = '1'
```

Figure 19: OpenEMR Logs Viewer

similar to OpenMRS, it does not allow restricting access to information on a per patient basis. One of its optional features is the "Patient Portal" which allows patients to access their medical information and communicate with their HCPs through the Web (OpenEMR Project Wiki, 2014).

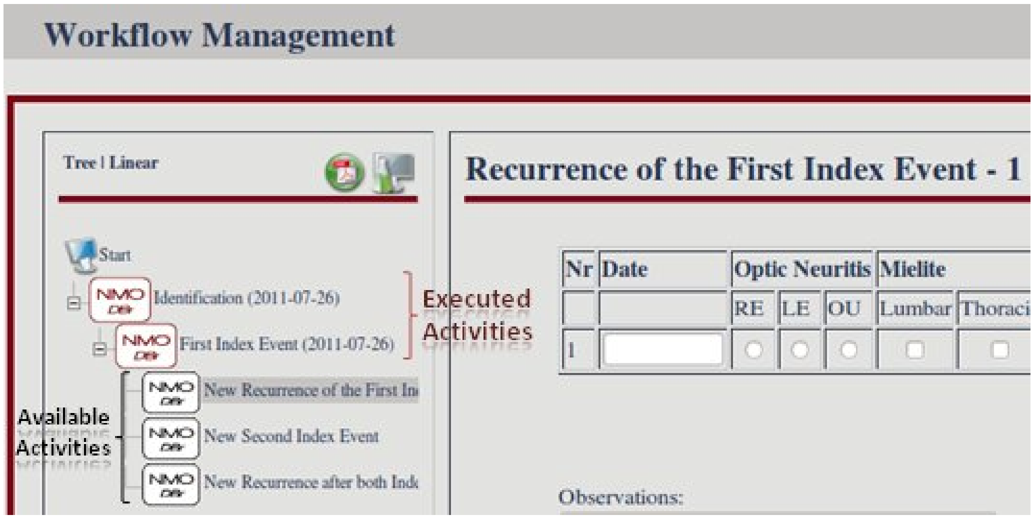
The existing logging and auditing mechanisms in OpenEMR were not comprehensive, do not ensure non-repudiation, and are modifiable by administrators making them untrustworthy (King et al., 2012). OpenEMR even bundles an embedded phpMyAdmin interface that allows administrators of the system to modify log entries from the system. As the OpenEMR logging mechanism just involves logging the SQL queries, this also means the logs viewable through this interface include the specific private information being updated or changed, such as what condition a patient has, increasing the risk of information exposure through logs (King and Williams, 2014). It does, however, include a warning to physicians when performing a limited number of actions that the action will be logged, such as when deleting information from the system. Examples of the log entries OpenEMR currently collects are shown in Figure 19.

6.1.4 FluxMED

FluxMED is a customisable EHR system designed to easily collect and manage different types of medical data (Faria-Campos et al., 2014). FluxMED enables medical specialists to customise the handling of different types of data in a specialised way without changes to its code. Data collected in the system is highly structured, and use of the system is defined in workflows. Each activity in the system is made up of events such as a consultation, an exam or test performed, with specific information included in attributes. FluxMED has been designed to be powerful and flexible by making it possible to standardise the types of data entered by defining them in a workflow. These can be changed easily, incorporating new knowledge without making changes to FluxMED's code. It can be used in very flexible ways, for example, if different doctors follow different diagnostic strategies, that is, ask different questions and request different exams, the workflow can incorporate both methods, and let the doctor choose which one to use. Data entered in this way is structured to make it easy to analyse it later. Data is not entered in free text format, but in formats that have fixed types and requirements, which simplifies posterior analysis.

Figure 20 illustrates how FluxMED can be used. Each step in the doctor's consultation, exams that have been requested, or any other relevant information is represented by an activity in a workflow. FluxMED presents the set of activities that have been executed, and the set of new activities that can be executed at any point. In Figure 20, two activities have been executed, Identification, and First Index Event. There are three new activities that can be executed at this point, shown in the second activity. In this case the user has selected the first of the new activities, and the right side frame shows the data that can be entered to register this activity. This example is taken from the NMO-DBr, the Neuromyelitis Optica Database, developed with FluxMED (Lana-Peixoto et al., 2011).

FluxMED has been used to develop EHR systems for three different diseases that are complex, difficult to diagnose and to treat. But because they are not common diseases, EHR systems aimed at them are non-existent or very difficult to access. FluxMED has been able to model data from patients of neuromyelitis


Workflow Management
Tree | Linear
Start
Identification (2011-07-26)
First Index Event (2011-07-26)
New Recurrence of the First In
New Second Index Event
New Recurrence after both Ind
Executed Activities
Available Activities
NMO DBr

Recurrence of the First Index Event - 1

Nr	Date	Optic Neuritis			Mielite	
		RE	LE	OU	Lumbar	Thoraci
1		○	○	○	□	□

Observations:

Figure 20: FluxMED NMO-DBr Workflow

optica, paracoccidioidomycosis and adrenoleukodistrofy and enable doctors to use the system to initiate and follow patient treatments.

An important aspect of the FluxMED system is that creating a workflow for a new disease takes only a few hours with the help of a medical specialist. There is no need to change the system in any way. Moreover, new systems can be integrated with existing ones, so one EHR system can serve several specialities, making it simpler to maintain the data, train users and extend the system.

FluxMED allows each activity to have a different set of access permissions, making it an ideal platform to illustrate the functionalities of IAF protocols with the ability to introduce fine-grained policies and accountability for each activity in a workflow. Patients, however, do not currently have a role in the system.

6.1.5 Selection

Table 5 includes a summary of the comparison between the different EHR systems on some of the key considerations. FluxMED was chosen for an implementation of the IAF protocols due to its highly structured worklows allowing us to know the context of activities in the system that deal with the eHealth data, while it currently lacks strong accountability mechanisms. As an implementation in a different type of system, I wanted to explore the implementation in a more standard EHR system with a normal RBAC approach to information access that I could augment with the IAF protocols. OpenEMR was chosen over OpenMRS because of its wider use in the US and other Western markets.

Table 5: Comparison of EHR systems considered

EHR system	**Use in similar countries**	**Typed data**	**Existing IA measures**	**Access control model**	**Patient role**	**Granularity of access**
HospitalRun	Aimed at use in developing world hospitals	No	No	RBAC	No	Access to all records per role
FluxMED	Currently in use in Brazil	Yes, with highly structured workflows	No	RBAC	No	Highly granular, with rules able to be defined in all steps of workflows
OpenEMR	Widely used in the US	Partial	Partial	RBAC	Yes, with extension	Per role or per a two-tier sensitivity label
OpenMRS	Focused on the developing world, not widely used in western nations	Partial	Partial	RBAC	Yes, via installable module	Access to all records per role

6.2 Case Study 1: OpenEMR implementation

As discussed in Section 6.1.3, OpenEMR is a widely used EHR system. While it has some existing audit and logging mechanisms in place, they have been found to be inadequate at this time. As a result of the state of logging and accountability within OpenEMR, I decided to make use of the services developed for the prototype in Chapter 4 for this implementation which also let us explore plugging in these services into an existing EHR system.

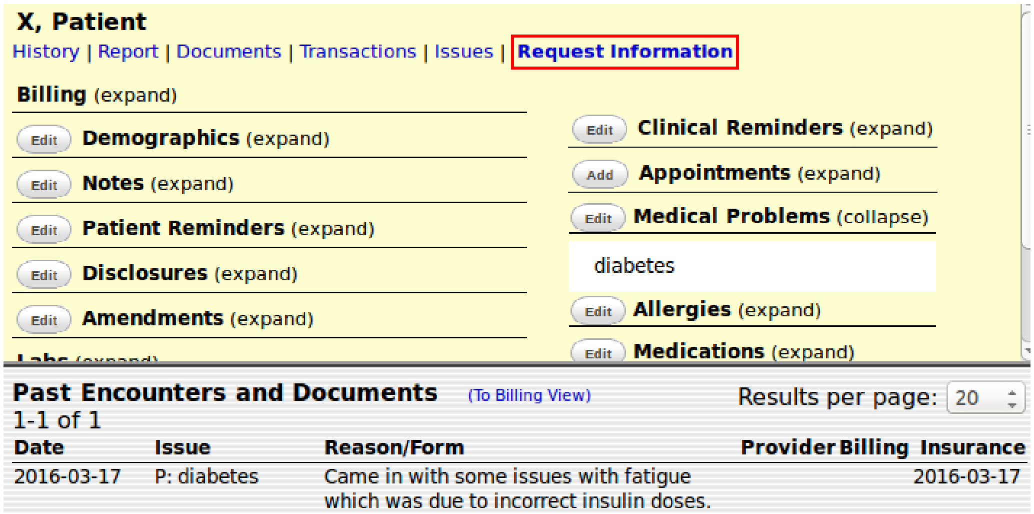
In this section, I demonstrate and discuss the implementation of the IAF protocols into OpenEMR.

6.2.1 Technologies

OpenEMR is written primarily in PHP with MySQL being used for the database. OpenEMR version 4.2.0 was used for the implementation, and it was run on the Apache web server on a Linux machine. The IA protocols were implemented into OpenEMR by calling the IAF prototype services developed in Chapter 4. OpenEMR was modified to additionally check the IAF services when performing an access control check and handle the response, including displaying warning messages when appropriate. The extra logging of event context and usage policies is handled from within the IAF services.

6.2.2 Implementing the protocols into OpenEMR

OpenEMR makes use of role-based access control and implements permissions with the PHP extension phpGACL (OpenEMR Project Wiki, 2012). This allows OpenEMR to assign permissions to roles, such as allowing users in the role *physician* to have access to *write* information to a patient's medical records. When integrating the IAF prototype services to augment this RBAC system, I added extra functions to run when the system checks these permissions. To simplify this for many cases in


X, Patient
History | Report | Documents | Transactions | Issues | Request Information
Billing (expand)
Edit Demographics (expand)
Edit Notes (expand)
Edit Patient Reminders (expand)
Edit Disclosures (expand)
Edit Amendments (expand)
Labs (expand)
Edit Clinical Reminders (expand)
Add Appointments (expand)
Edit Medical Problems (collapse)
diabetes
Edit Allergies (expand)
Edit Medications (expand)
Past Encounters and Documents
(To Billing View)
Results per page: 20
1-1 of 1

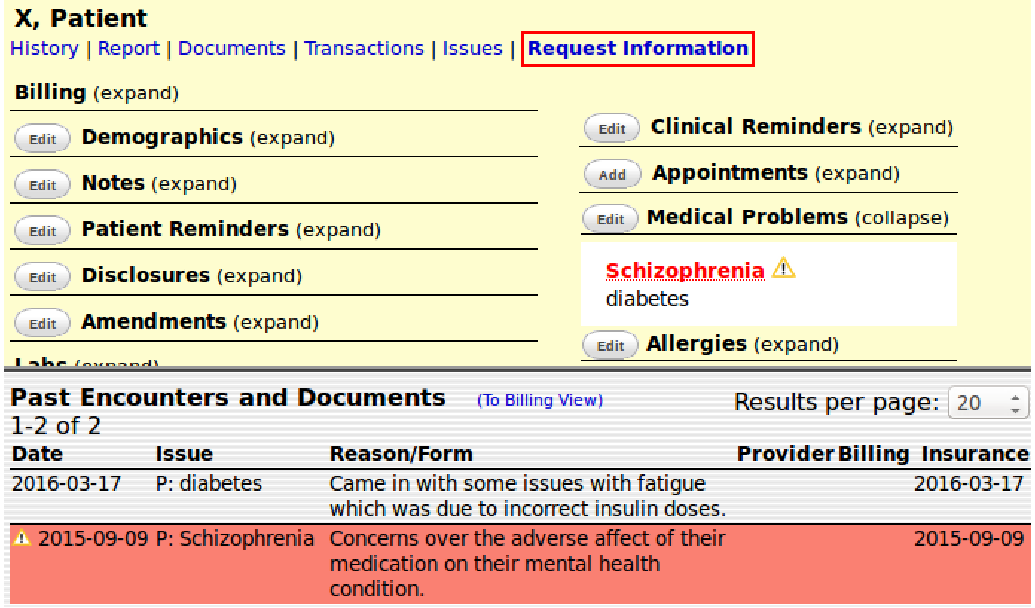
Date	Issue	Reason/Form	Provider	Billing	Insurance
2016-03-17	P: diabetes	Came in with some issues with fatigue which was due to incorrect insulin doses.			2016-03-17

Figure 21: The patient summary before requesting access to mental health history

the system, I was able to write a wrapper around phpGACL's main entry point, the `acl_check` method, that was passed more information about the type of information being accessed and performed the extra checks for the IAF by calling the usage query service.

OpenEMR allows providing the types of information such as diagnoses using imported tables of types such as ICD-9. This is not enforced by the interface however, and having a type for each piece of data is an important requirement for being able to define and enforce usage policies and rules as part of the IAF protocols. When a HCP is adding to the patient encounter history to provide a summary of a patient visit, the context of the visit can be provided such as an "Office Visit" and the summary of the visit can be linked to an existing medical problem. This linking of the encounter history to the medical problem is useful when a type is enforced, as the system can then decide if that patient history entry is able to be viewed or modified. The HCP can also specify if the entry is of high sensitivity which can be used in combination with the type of information to reason about access to the information.

Other changes also needed to be made in order to display extra information in the interface when the IAF call resulted in an action being restricted and to

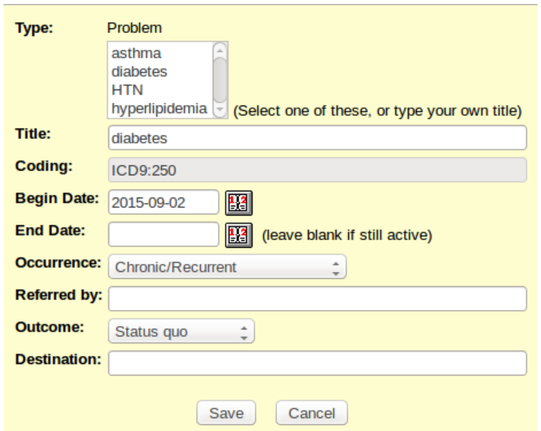

X, Patient
History | Report | Documents | Transactions | Issues | Request Information
Billing (expand)
Edit Demographics (expand)
Edit Notes (expand)
Edit Patient Reminders (expand)
Edit Disclosures (expand)
Edit Amendments (expand)
Labs (expand)
Edit Clinical Reminders (expand)
Add Appointments (expand)
Edit Medical Problems (collapse)
Schizophrenia ⚠
diabetes
Edit Allergies (expand)
Past Encounters and Documents
(To Billing View)
Results per page: 20
1-2 of 2

Date	Issue	Reason/Form	Provider	Billing	Insurance
2016-03-17	P: diabetes	Came in with some issues with fatigue which was due to incorrect insulin doses.			2016-03-17
⚠ 2015-09-09	P: Schizophrenia	Concerns over the adverse affect of their medication on their mental health condition.			2015-09-09

Figure 22: The patient summary after requesting access to mental health history

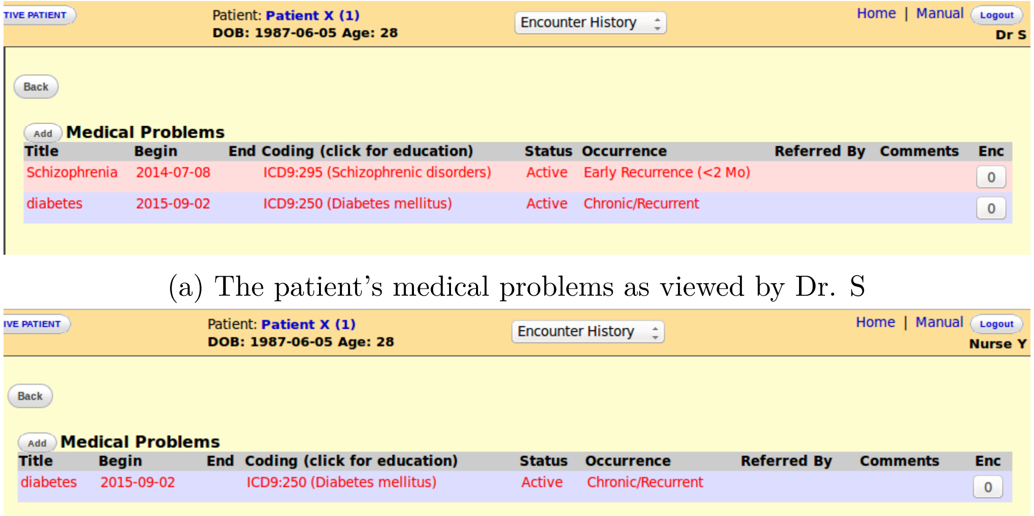
allow HCPs to override a patient preference when needed. This was a challenge as OpenEMR presents most information in a basic summary form, so I needed to add a way for HCPs to request information types that may currently be restricted. This was done by adding a “Request Information” link at the top of the patient summary view, which leads to a new form to make the information access request. The web front-end from the IAF prototype was used for managing access and submitting and responding to inquiry requests rather than building a new interface for this purpose within OpenEMR.

The scenarios described in Chapter 4 were used as a way to verify and demonstrate the functionality of the implementation in OpenEMR. For example, suppose a doctor has been restricted from accessing their patient’s mental health history but determines they need to access the patient’s mental health history before prescribing a medication. To enable this, the HCP can use the “Request Information” link at the top of the patient summary view. By entering the type of information into the resulting form, they will receive a warning that they are restricted from accessing this information due to the patient’s policy, but can proceed with accessing it if needed



Type:	Problem asthma diabetes HTN hyperlipidemia (Select one of these, or type your own title)
Title:	diabetes
Coding:	ICD9:250
Begin Date:	2015-09-02
End Date:	(leave blank if still active)
Occurrence:	Chronic/Recurrent
Referred by:	
Outcome:	Status quo
Destination:	

Figure 23: Adding a diagnosis in OpenEMR



Patient: **Patient X (1)**
DOB: 1987-06-05 Age: 28

Dr S

Medical Problems

Title	Begin	End	Coding (click for education)	Status	Occurrence	Referred By	Comments	Enc
Schizophrenia	2014-07-08		ICD9:295 (Schizophrenic disorders)	Active	Early Recurrence (<2 Mo)			0
diabetes	2015-09-02		ICD9:250 (Diabetes mellitus)	Active	Chronic/Recurrent			0

(a) The patient's medical problems as viewed by Dr. S

Patient: **Patient X (1)**
DOB: 1987-06-05 Age: 28

Nurse Y

Medical Problems

Title	Begin	End	Coding (click for education)	Status	Occurrence	Referred By	Comments	Enc
diabetes	2015-09-02		ICD9:250 (Diabetes mellitus)	Active	Chronic/Recurrent			0

(b) The patient's medical problems as viewed by Nurse Y

Figure 24: Medical problems view under different policies

for the given purpose. A notice is also given that the action will be logged and the patient notified. Upon confirming this access request, the doctor will be returned to the patient summary with the restricted information now displayed in a different colour as shown in Figures 21 and 22.

I have further implemented the requirements for delegated access defined in Chapter 5 to demonstrate their functionality in OpenEMR. The delegation of access from the patient perspective is implemented in the IAF prototype and managed through the existing prototype Web front-end. However, I needed to implement the access delegation for HCPs so that it would work within OpenEMR. To depict Scenario 3 in the OpenEMR, I define a usage policy by the Physician “Dr. S” to delegate access to “Nurse Y” to add entries to a patient’s record, but only to be able to view entries that they created. This is accomplished by augmenting OpenEMR’s access control mechanisms. The system first matches the usage policy’s append-only constraint to OpenEMR’s ‘addonly’ permission, then it augments the ‘view’ permission to restrict which information is viewable. Each action is logged along with the usage policy that was used at the time.

In the scenario, Nurse Y adds information about Patient X’s new diagnosis of diabetes as shown in Figure 23. The patient has previously been diagnosed with schizophrenia. Upon submitting the new diagnosis the Nurse is able to view it under the patient’s medical problems, but cannot view the schizophrenia diagnosis, while Dr. S can view both as shown in Figure 24.

The implementation of the IAF protocols in OpenEMR has demonstrated that the protocols can be successfully implemented into an existing EHR system. The services developed in Chapter 4 were able to be used to augment the role-based access control system used by OpenEMR. However, we also saw that existing systems have a long way to go toward IA, as a number of changes had to be made to the system for this to be accomplished and the existing auditing facilities were found to be insufficient despite OpenEMR being HIPAA compliant.

6.3 Case Study 2: FluxMED implementation

As discussed in Section 6.1.4, FluxMED is a customisable EHR system designed to easily collect and manage different types of medical data. Due to the flexible nature of FluxMED’s workflows and activities, we decided to try to experiment with implementing the IAF protocols natively into FluxMED rather than use the services prototype from Chapter 4. This would both let us explore implementing the protocols natively into an existing EHR system, and let us create a more complex implementation required to maintain FluxMED's existing flexibility.

In this section, we will demonstrate and discuss the implementation of the IAF protocols into FluxMED. This implementation was conducted in collaboration with Sergio Campos and Paulo Batista who work on FluxMED at the Universidade Federal de Minas Gerais in Brazil. In this collaboration, I provided the specifications, guidance, and feedback for how to implement the protocols, while Paulo Batista undertook the actual implementation work into the FluxMED system. Likewise, for the pilot study with HCPs discussed in Section 6.4, I devised the questions to prompt the discussions while the actual interviews were conducted by Sergio Campos and Paulo Batista with the anonymised data from these interviews made available on request to any researcher which I subsequently analysed.

6.3.1 Technologies

FluxMED is written in Java on the server side with MySQL used as the data store. The IAF protocols were implemented natively into FluxMED rather than using the services prototype. The policies and logs were both stored in the relational database similar to the recorded data.

6.3.2 Implementing the protocols into FluxMED

In FluxMED, an EHR system is developed by describing the steps in the HCPs' consultation and treatment, and their attributes. For example, Figure 20 presents a screenshot of NMO-DBr, the Brazilian Neuromyelitis database. In this case, the HCP examines their patients by first identifying them through their name, address, and other information. This data is stored in the first activity of NMO-DBr. Once a patient is identified, the doctor can store what is called the First Index Event. This disease is rare and difficult to diagnose. Doctors establish their diagnosis by

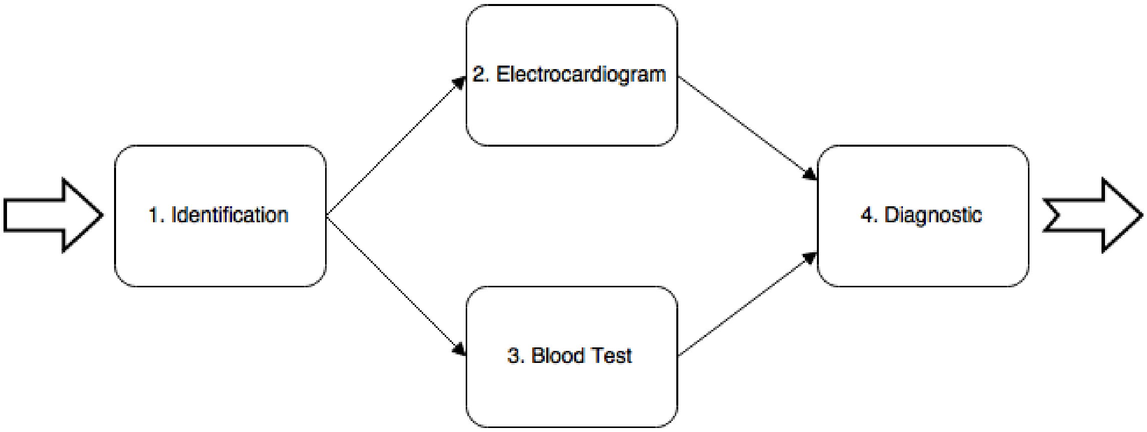


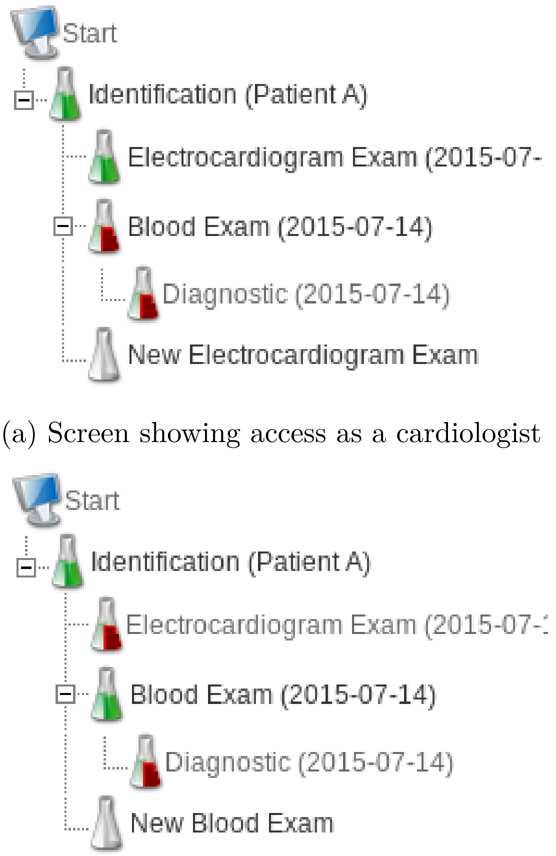
Figure 25: A simple workflow illustrating IA in FluxMED

identifying what type of problems patients have, and if a certain number of crises occur the disease is completed. Each crisis is called an Index Event. Several index events can occur, and NMO-DBr can store all of them and maintain their temporal relationship.

An EHR system inside FluxMED is a series of activities, each recording an aspect of the patients' symptoms and treatment. Symptoms and consultations can be stored as separate activities in FluxMED, as well as exams and treatments. The doctors using FluxMED then see the sequence of activities that have been registered, and can view each of them by selecting the activity name as seen in the left frame of Figure 20.

FluxMED's access control system grants access permissions on a per activity basis. An example of usage could be if you have four activities: 1. Identification; 2. Electrocardiogram exam; 3. Blood exam; 4. Diagnostic. Activities 2, 3 and 4 can only be executed after activity 1. Figure 25 shows how FluxMED sees this example.

In order to implement the IAF protocols into FluxMED, its permissions system must support both basic allowing or denying certain actions on each activity as it did previously, and the IAF approach for more complex access and usage policies. In order for FluxMED to remain flexible, this is a complex task as a lot of parameters must be configurable and tested in order to maintain interactions between existing


Start
Identification (Patient A)
Electrocardiogram Exam (2015-07-
Blood Exam (2015-07-14)
Diagnostic (2015-07-14)
New Electrocardiogram Exam
Start
Identification (Patient A)
Electrocardiogram Exam (2015-07-1
Blood Exam (2015-07-14)
Diagnostic (2015-07-14)
New Blood Exam

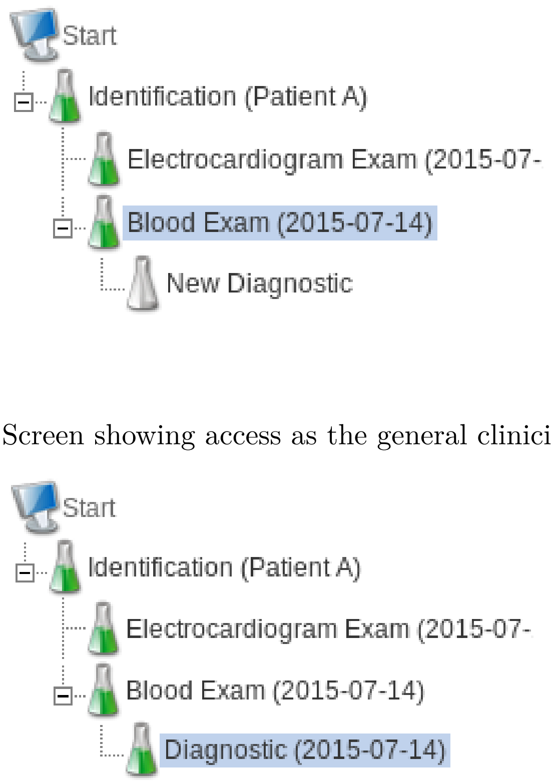
(a) Screen showing access as a cardiologist

(b) Screen showing access as laboratory technician

Figure 26: Screen behaviour under different roles

business rules. IA is implemented in FluxMED by assigning access permissions to each activity according to who can access the records based on usage policies. An example of this could be if a policy states that Activities 1 and 4 can only be executed by a general clinician. As shown in Figure 26, cardiologists can view Activity 1 and execute Activity 2, lab technicians can view Activity 1 and execute Activity 3, and the general clinician can view all activities. In this way, the general clinician can view all exams and make the diagnosis. Cardiologists and lab technicians can view the identification so they will know who to examine. They will be able to register their exams, but will not see exams performed by other personnel.

Finally, the complete set of activities, called an instance in FluxMED, has the patient as the owner who can see all four activities and change permissions for their


Start
Identification (Patient A)
Electrocardiogram Exam (2015-07-
Blood Exam (2015-07-14)
New Diagnostic
Start
Identification (Patient A)
Electrocardiogram Exam (2015-07-
Blood Exam (2015-07-14)
Diagnostic (2015-07-14)

(a) Screen showing access as the general clinician

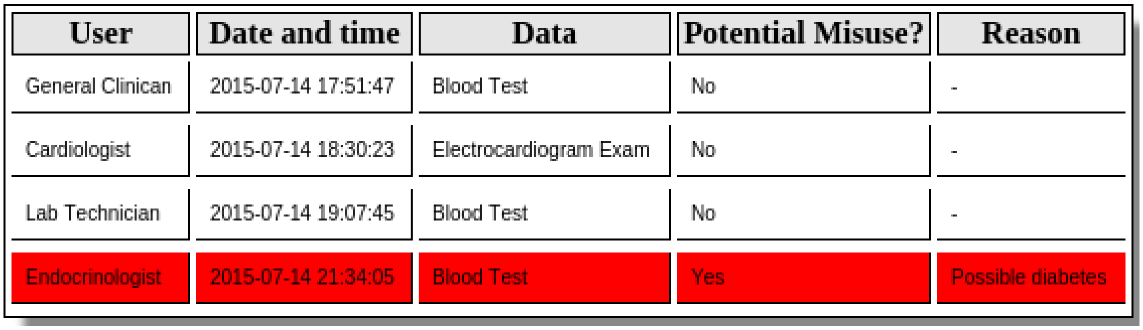
(b) Screen showing access as the data owner, or the Patient A

Figure 27: Screen behaviour under different roles

data.

FluxMED registers all access activity in the system. Each execution or modification of an activity is registered. In addition to that, activities visualisation is also registered. So, if a user chooses to visualise an activity, this fact is also registered in the system, so the patient can see a full history of which doctors and other healthcare professionals accessed their data, if the HCP had enough privileges to see this information as seen in Figure 28.

FluxMED has proven a useful test case for the implementation of the IAF protocols natively in an EHR system. Its flexible but highly structured approach to accessing and adding health data was both challenging and a powerful use case for fine-grained policies possible with the IAF protocols.



User	Date and time	Data	Potential Misuse?	Reason
General Clinican	2015-07-14 17:51:47	Blood Test	No	-
Cardiologist	2015-07-14 18:30:23	Electrocardiogram Exam	No	-
Lab Technician	2015-07-14 19:07:45	Blood Test	No	-
Endocrinologist	2015-07-14 21:34:05	Blood Test	Yes	Possible diabetes

Figure 28: Possible information misuse are highlighted in FluxMED

6.4 Views of healthcare professionals on IA in FluxMED

To understand the opinions of healthcare professionals who used FluxMED towards the implementation of the IAF protocols and the IA approach to access control by patients, interviews were conducted with five medical researchers. This will serve as a pilot study on the views of healthcare professionals on the use of the IAF protocols in real-world EHR systems.

6.4.1 Participants and Methods

The interviews were conducted with five doctors, including cardiologists and neurosurgeons, who were also researchers at the Universidade Federal de Minas Gerais in Brazil. The interviews were conducted by Sergio Campos and Paulo Batista—two researchers at the university—and the anonymised interview data was made available on request to any researcher which we are using for analysis.

The doctors were first walked through the IAF protocols and concepts in a presentation prepared by Sergio Campos and Paulo Batista in Portuguese. The presentation involved examples from a high fidelity prototype of FluxMED implementing the IA protocols, which were used to explain the functionality of the accountable FluxMED system from the doctor's perspective. A semi-structured interview was then undertaken. The main topics for discussion in the interviews were whether the doctors feel the IAF approach and protocols balance their need for access to the information against the patients desire for control of their private information and transparency into how it is used, as well as their views are on what type of information patients should be able to view about their own record, and the doctor's perspectives on the implementation of the IAF protocols.

6.4.2 Results and Discussion

The doctors interviewed did not, in general, feel uncomfortable with the IAF protocols and considered it a good step forward. They were all positive about the accountability mechanisms and felt it was important that all accesses to data was auditable and that it is possible to trace who accessed what information at all times.

The participants were positive about the use of both the IAF protocols and FluxMED and felt it could be a significant contribution because there is currently not an efficient flow of information between the different levels of healthcare, i.e. information obtained in primary care does not go to secondary care, and information from secondary care does not go to tertiary care. They felt that the way the IAF protocols approach restricting information access would be useful in these cases, allowing one doctor to pass information to the next doctor, while maintaining some control over the information.

Two of the participants stated they believe that using the IAF as part of the access control approach to eHealth information has the potential to remove barriers to using EHR systems, due to it providing assurances that data is not misused which is a common concern. They commented that if well implemented, the use of IAF protocols could help make the use of EHRs more acceptable, and as a result increase their usage.

The participants were positive about the aspects of patient control in the IAF protocols. They pointed out that it was important that patients could ensure only the doctors they were seeing had access to their information, and that patients should be able to restrict access to their records from specific professionals, such as doctors they no longer trust.

Some of the doctors did have the opinion, however, that they did not see a great need to be able to restrict information from certain doctors, but felt it was important to be able to restrict information from being accessed by other professionals such as social workers and nurses. As an example given, two of the doctors worked with genetic diseases that are rare, but they are rather common among the affected families. Many of these patients live in small towns, where local doctors and health workers are not specialists in the diseases. So, for these workers, access to basic information would be valuable, because they would be able to help others in the family, but not necessarily detailed information about specific patients.

The complexity of the IAF protocols with the different levels of healthcare was discussed with the five doctors. It was pointed out by the participants that for it to be implemented and used consistently, it would require approval from all levels of health services. In the Brazilian environment, healthcare professionals can work for private institutions, as well as state, city and federal hospitals. To maximise the benefits of sharing information and ensure that a doctor in the middle of treatment chain can access the information appropriately, all levels of healthcare would need to approve the use of the protocols. The doctors felt that making it possible to guarantee access to the right medical information to the right people in a way that the health system would trust it was a significant contribution.

Additional comments were made by the participants about the potential for the IAF protocols to be used by healthcare institutions to define policies on what information can be shared between them and in what circumstances, while providing accountability. One example given by a participants was that it can be the case in Brazil where a hospital or other institution is legally responsible for the data and cannot pass all the information to other hospitals. The participants felt that with the

IAF protocols implemented, policies for sharing specific data can be introduced that would ease the process of regulating such sharing of information. A hospital may be granted permission, for example, to share anonymised ECGs to another hospital, but existing EHR systems would make the anonymisation requirement complex. If the IAF was in place, it would much easier to guarantee that only the parts of the data that can be shared will be, which the participant believed could help ease the adoption of EHRs. The health data providers setting policies on how their data is shared and used is a use case I discuss in Chapter 7.

6.5 Discussion

The initial review of open source EHR systems discussed in Section 6.1 found that IA is lacking in the most widely used open source medical record systems. From the two implementation case studies, it was found that neither OpenEMR nor FluxMED had existing measures that were sufficient for the level IA required by the IAF protocols.

When implementing the IAF protocols into OpenEMR and FluxMED, two different approaches were taken. In OpenEMR the services of the IAF prototype initially developed and discussed in Chapter 4 were used to plug in the IAF protocol functionality by modifying OpenEMR to call out to the services when needed. In the FluxMED study, the IAF protocols were implemented natively within the FluxMED code base. The OpenEMR implementation was simplified by wrapping its main access control method with extra functionality for the IAF. The use of the services to add the IAF protocols to the system was efficient and worked effectively with some small modifications to OpenEMR. This also ensured that the IA requirements for logging and accountability did not have to be reimplemented. The implementation natively into FluxMED was more complex, particularly with the need to maintain the interactions between existing business rules. The use of a native implementation provided flexibility in the implementation with the complex FluxMED workflows, but results in increased development time.

In comparing the two systems, FluxMED could be seen as providing a better platform for the use of IAF protocols due to the highly structured nature of the workflows and data in the system. OpenEMR did allow for structured information, however, ensuring the consistency of the information types was problematic. OpenEMR also needed a lot of modifications to its interface to make it possible for HCPs using the system to receive warnings, override patient preferences, and request access to information types that may currently be restricted. FluxMED's highly structured workflows allowed for more fine-grained implementation of the IA protocols. The flexible and configurable nature of the workflows made for a more complex implementation of the protocols, however, the result allows for highly granular usage policies that can be used in the workflows to maintain accountability.

6.6 Conclusion

In this chapter, I have explored the implementation of the IAF protocols into two existing EHR systems, OpenEMR and FluxMED, as case studies. It was found that the evaluated eHealth systems did not have existing accountability mechanisms that provided non-repudiation and active auditing for misuse.

Through the implementations in OpenEMR and FluxMED, I have demonstrated that it is possible to modify existing systems to support the IAF protocols. Two different approaches were taken, with the services from Chapter 4 being used to plug in the IAF functionality into OpenEMR, while the protocols were implemented natively in FluxMED. The use of the services in the OpenEMR implementation led to simplifying the implementation and separate the functionality into cleaner components. While this was suitable for a system with a more straightforward approach to accessing and entering information, in a complex and flexible system such as FluxMED, a native or more custom implementation of the protocols is more suited in order to maintain the systems requirements and flexibility. For OpenMRS which was also considered in Section 6.1, a similar approach to the one taken in OpenEMR would be possible in order to implement the IAF, providing a solution to enforce strict data types for the health information are in place. HospitalRun on the other hand does not currently allow data types as of the time of the evaluation, making it difficult to apply usage policies and implement the protocols fully.

OpenEMR had challenges in enforcing that information entered had an appropriate type associated with it which could be used to compare access to it against usage policies. This was not solved in this work, but as OpenEMR does allow entering types for data, it would be possible to modify the system to enforce this condition enabling an implementation to succeed.

Between the two implementations, FluxMED was found to provide a better platform for implementing the IAF protocols due to its highly structured approach to data while allowing flexible workflows for different situations. However, this also led to more complexity during the implementation.

A pilot study into the views of healthcare professionals on the use of the IAF protocols in FluxMED was conducted by our research partners in Brazil, Sergio Campos and Paulo Batista. From these interviews, the participating doctors were positive about the potential of the IAF protocols and provided valuable insight into the possibilities and challenges of implementing such a system in the Brazilian context.

These implementations into existing EHR systems provide the groundwork for future work on implementing the IAF protocols and AeH systems in real world situations. Future work could include making use of the implementation in systems such as FluxMED to further validate and investigate the use of the IAF and AeH systems. This future work could involve the use of a "shadow" implementation where the modified system logs the actions it would have taken in a given situation due to the IAF protocols without initially changing the behaviour of the system for

HCPs using the system. This would permit the evaluation the IAF against actual user traffic in a non-invasive manner. It is also important that we can evaluate ways to make the creation of the default policies and rules for misuse scalable. It may be useful to explore creating implementations that use data such as how many times a policy needs to be overridden and in which situations that occurs to suggest improvements to rule sets.

In the next chapter, I discuss and explore the application of the IAF protocols into decentralised eHealth systems.

7 Applying the IAF to decentralised systems

The initial model of the IAF was designed for use in shared eHealth Record and local EHR systems which are centralised. The application of the protocols to decentralised systems, with data distributed among many healthcare providers and other data sources has not been addressed. Decentralised data sources in eHealth are common and information is often distributed in data silos.

In this chapter,[5] the possibility of supporting greater sharing of information while respecting patient privacy preferences through a consent model and ensuring accountability for the information users is investigated. I explore modifications to our Information Accountability model and Framework to provide a modified IAF model that is applicable to decentralised systems. This is preliminary work and there is scope for future research into the use of the IAF in decentralised systems.

7.1 Decentralised systems

In the US alone, it is estimated that healthcare data had reached 150 exabytes in size by 2011 (Cottle et al., 2013), and it is believed countries with large populations such as India and China could soon be handling zettabyte and yottabyte scale data (Andreu-Perez et al., 2015; Cottle et al., 2013). With the large growth in this health information from the variety of medical systems and sources, there comes significant issues such as interoperability and the creation of data silos (Richesson and Chute, 2015). To protect patient privacy, health data is often scattered and intentionally isolated among institutions (Weber et al., 2014).

In addition to EHRs maintained by hospitals and local healthcare providers, there are an increasing number of heterogeneous distributed healthcare data sources that could provide additional information that could be used to drive clinical decision making and improve the quality of care (Marcos et al., 2015; Wood et al., 2015).

[5] Publications related to this chapter: Grunwell and Sahama (2015a)

These data sources can include sensor data obtained from monitoring patients and patient generated health data. This may be recorded by patients manually or collected by the various consumer devices (e.g. phones, smart watches, and fitness wristbands) and includes their vital signs, physical activity, sleep patterns, and medications (Wood et al., 2015). With information commonly distributed among many hospitals and medical systems, a patient's health information is decentralised. In addition to aggregating information into a shared EHR, we must also consider the need to share information among institutions and systems.

To increase the availability of the eHealth information at the point of care, the various producers of this health information must share the data. However, this will raise patient privacy concerns and mechanisms for patients to consent to their information being shared and used are required. Weber et al. (2014) states that there is a need for a consent mechanism that can enable patients to "decide how and when their data can be shared with or "mashed up" against other databases." The Information Accountability Framework we have proposed could be modified to address this need.

The need to provide for sharing between health institutions was highlighted in the pilot study with healthcare professionals in Brazil in Section 6.4. In cases such as in Brazil's healthcare system, a hospital or other institution is legally responsible for the data and cannot share all of the information with other hospitals. In such circumstances, allowing healthcare institutions to define policies on what information can be shared between them and in what circumstances, while providing accountability, has the potential to ease the adoption of the sharing of EHR information. With the IAF approach, policies for sharing specific data can be introduced so that organisations can guarantee that only the parts of the data that can be shared will be. This is a use case in which we believe the IAF model has potential to enable the sharing of information while maintaining accountability.

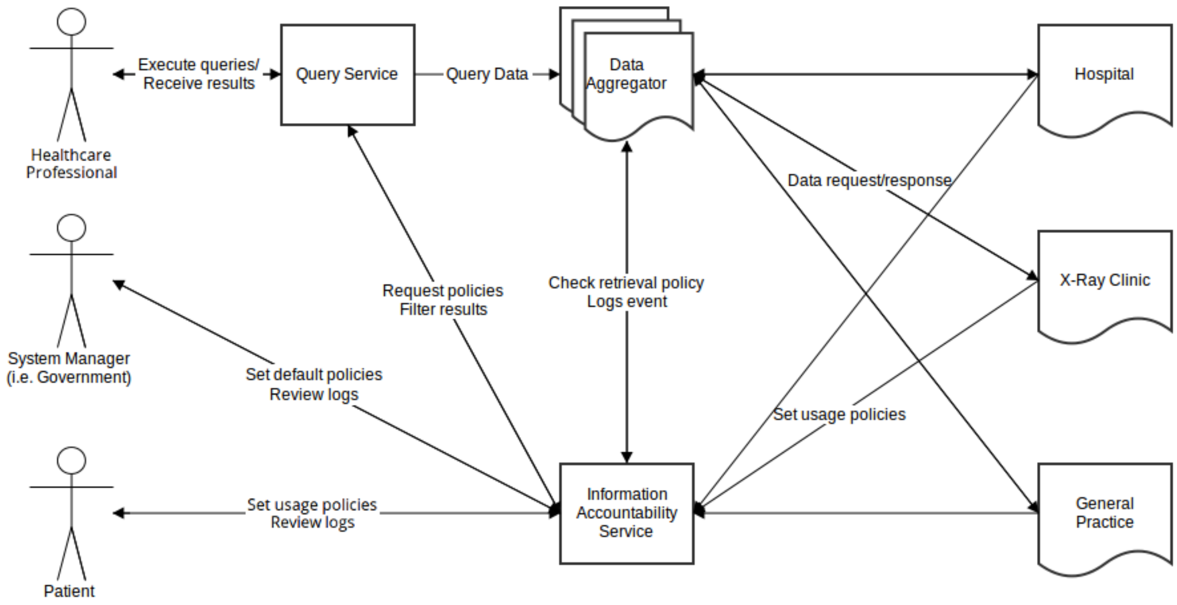

Healthcare Professional
Execute queries/ Receive results
Query Service
Query Data
Data Aggregator
Hospital
Data request/response
System Manager (i.e. Government)
Request policies Filter results
Check retrieval policy Logs event
X-Ray Clinic
Set default policies Review logs
Set usage policies
Patient
Set usage policies Review logs
Information Accountability Service
General Practice

Figure 29: Information accountability model for health decentralised systems

There have been other approaches to privacy protection of decentralised health data. Weber-Jahnke and Obry (2012) developed a consent management mechanism to preserve privacy in systems that allow the peer-to-peer exchange of medical information. This approach also involved allowing overrides of patient consent restrictions in emergency situations. Seneviratne and Kagal (2014) proposed creating a new web protocol, accountable HTTP, that would provide provenance trails for the transmission of data and media on the web through a network of provenance trackers. Data owners would be able to set policies and audit the transmission of their information after-the-fact. These approaches differ from ours where we include a HA guaranteeing legitimate HCPs have appropriate access to the relevant information when they need it, provide proactive detection and notification of potential misuse, deter HCPs from misuse, and allow patients to submit inquiries and interact with HCPs to resolve disputes. However, aspects of these approaches could be applied in combination with the IAF protocols.

7.2 Applying the IAF to a decentralised process

The initial IAF model focused on patient control of their information in a central location. In a distributed setting, to encourage the sharing of health information between different data owners and institutions, we must ensure that the providers of the information are considered in defining how the information can be used and shared.

In order to reap the benefits of shared eHealth information systems and encourage the sharing of information through providing transparency and accountability to information usage, we have devised a model the sharing of eHealth information that makes use of the principles of the initial Information Accountability Framework. The initial model focused on patient control, but for the purposes of information sharing, we must also consider the view point of the producers and providers of eHealth information as stakeholders in the collection and use of this data.

In the modified IAF model for decentralised use cases, patients would be able to explicitly consent to whether or not their data could be shared or aggregated. Through accountability mechanisms, they would always be informed how and why their information as being queried and used by HCPs. In the devised information accountability model for sharing eHealth data, healthcare professionals and other producers of eHealth information—including the patients themselves—are also able to specify policies for how the information they produce can be aggregated, shared, and used. These policies are then combined with patient policies and policies set by a governing Health Authority to determine which information is permitted to be aggregated or shared for that patient from that data source. The HA policies would ensure that the aggregation and sharing policies set by providers do not restrict sharing information that is essential for providing appropriate care, and in a national system it would be the role of government policies to ensure providers do not unduly withhold information. The process for this model is demonstrated in Figure 29 which uses an example with a central system, designated as a “Data Aggregator”, facilitating the sharing of information between HCPs and data providers, applying usage policies, and monitoring for misuse.

I define four different types of users to demonstrate this model:

- **Data Owners:** Data owners refers to the individuals to whom the data refers to, i.e. patients.
- **Data Providers:** Data providers refers to the groups and individuals who produce and/or store the information that will be aggregated. Data providers could be various types of healthcare providers such as hospitals, general practitioners, an X-ray clinic, etc. or it could be patients through manually entered data or data generated by systems such as mobile health applications
- **System Manager:** A system manager refers to the organisation responsible for maintaining the shared eHealth information system, and setting appropriate policies and investigate potential misuse. This could be a government department.
- **Data Users:** Data users refers to those who would make use of the shared or aggregated data, i.e. healthcare professionals.

7.2.1 Setting policies

Data providers

Data providers (i.e. hospitals, specialists, patients, etc.) are able to opt-in to sharing their data and set usage and aggregation policies on the information they produce. For example, a general practice may be willing to share condition and medication summaries about patients, but not detailed notes made by the patients’ doctor. A policy depicting this example is represented in ODRL in Listing 5, which

```
<o:policy xmlns:o="http://odrlextension.org/ns/odrlx/2x" xmlns:eh="
   urn:ehealth.gov" type="http://odrlextension.org/ns/odrlx/2x/
   privacy" uid="policy-use-ehr">
  <o:permission>
    <o:asset uid="urn:ehealthSystemData:11986" relation="o:target"/>
    <o:asset uid="urn:ehealthSystemData:11986" relation="x:collection
       "/>
    <o:party uid="urn:healthProfessional:10946" role="o:assigner"/>
    <o:party uid="urn:ehealthSystem:1458" role="o:assignee"/>
    <o:action name="o:aggregate"/>
    <o:constraint name="o:dataType"
        operator="o:isAnyOf"
        rightOperand="eh:prescription
          eh:conditionSummary"/>
  </o:permission>
</o:policy>
```

Listing 5: Example aggregation policy for a general practice represented in ODRL

shows the ‘aggregate’ action being permitted on data matching the prescription and condition summary types.

Data owners

Data owners (i.e. patients) are able to opt-in to having their data shared and aggregated through usage policies on their information. Patients maintain control over who has access to their information and in which contexts.

System manager

System managers who oversee the shared eHealth data system, such as a government’s health department, set default policies and restrictions on data collection and use.

7.2.2 Data aggregation

In the model, a central system referred to as a data aggregator collects information from the data providers. While doing so, it queries the IA service to retrieve an aggregation policy set made up of data owner and data provider preferences in order to ensure it only aggregates permissible data and avoids patients who have not opted-in to their data being shared.

7.2.3 Querying data

When a data user executes a query in the system, the query service retrieves a policy for the data user which is amalgamated from the policies of the data owner, data provider, and HA. This can include rules regarding which data they can access and how they can use the data.

If the data user is permitted to perform the query, the retrieved rules are then applied to filter the result set, removing restricted information. The information access request is logged, and the policy versions used to determine the access request is stored with the context-aware log entry.

7.2.4 Access to logs

As previously discussed in Section 5.2, the logs produced in an accountable system can contain sensitive information themselves. It is critical that the logs must be appropriately protected, including restricting who can view these logs and for what purpose.

Data providers

Data providers can view log summaries of when and what information they provided was aggregated and shared. The logs maintained by the accountability mechanism can also be used for risk management. If information originating from a data provider is found to have been misused or leaked, they can verify who accessed their information aggregated in the system.

Data owners

Data owners can view the log entries for their information. They can review these logs at any time, and submit inquiries for events identified as potential misuse.

Data users

Data users will be able to access specific log entries regarding their own access to patient information. They will be able to review the entries when they receive an inquiry requesting that they justify why they needed to access the relevant information in the given situation.

System manager

The system manager will be able to view all logs and provenance information for the aggregated data. This is necessary for the purposes of investigating potential misuse detected by the system. They will also need to be able to verify the integrity of the log entries and usage policies.

7.3 Implementation challenges

Many challenges remain to be investigated in order implement the proposed IAF model when accounting for decentralised use cases.

7.3.1 Scalability and performance

At the scale of a state or national health system, the amount of data collected can be considered Big Data. When performing queries at the scale of big data, the complexity of the queries can result in superexponential growth in computing time as the data set increases (Kuo et al., 2014). With that in mind, it is still important that additional access and privacy controls applied when querying data can scale. In producing a prototype of this model, the efficiency of applying these controls to filter and present results must be considered, as well as techniques for minimising their effects.

As the most common Big Data analytics approach is the use MapReduce systems such as Apache Hadoop, a possible solution to this problem lies in current research around providing fine-grained access control in MapReduce systems with low overhead (Ulusoy et al., 2014). GuardMR, as an example, allows the application of security policies to dynamically create authorised views of the data (Ulusoy et al., 2015). The amalgamated IAF policy for the user at the time of querying could be used to similarly efficiently create authorised views of the data.

7.3.2 Log storage and presentation

To provide accountability, appropriate provenance information must be stored and verifiable. In a query of a shared record pulled from many data sources, the results must generate policy-aware provenance information that can be used to verify how, why, and when a piece of information was accessed. This creates a challenge of how to efficiently store such data while maintaining privacy and security of the information they contain, as the logs themselves can contain sensitive information, as discussed in Section 5.2. Likewise, a principle of accountability is the transparency of the information use to data owners. The presentation of this information to patients so they can view who accessed their information and under what conditions provides additional scalability and usability challenges.

When HCPs access health information on individual patients in a centralised system, the presentation of this information can easily be handled. However, when data about patients is accessed that is decentralised among many data providers, this creates a challenge of how best to store and present the provenance information. A possible solution to this is to store both the detailed individual logs and generate summary views of the data accesses that are more meaningful to patients and providers when auditing access to their information.

7.3.3 Data heterogeneity

The diverse systems that produce health data provide data in various formats. As such, the heterogeneity of the data is a major challenge for the sharing and aggregation of information (Kuo et al., 2014; Marcos et al., 2015). To provide accountability, the framework must be able to match up data types of the information to those used to define policies, presenting a challenge of how to normalise the aggregated data.

A possible solution to this is to include a data integrator step when aggregating the data from the heterogeneous sources (Kuo et al., 2014). In this step, rules to match various data types, terminologies, and structures to transform them to a standard structured format that can be understood by the IAF mechanisms when applying policies for access to the information.

7.4 Conclusion

An increasing volume of health information is generated from many different systems. Increased sharing of health information between healthcare institutions and other health data providers could lead to greater availability of information at the point of care and improved decision making. However, concerns over patient privacy have hindered the sharing of information between institutions and the aggregation of data from the various sources of eHealth information.

In this chapter, I proposed a modified IAF model to address the privacy concerns for sharing and combining of health data through a patient consent based approach. In the IAF model applied to these decentralised use cases, patients are able to decide how and when their data can be shared with other healthcare institutions and HCPs, while maintaining accountability and transparency. Additionally, the model aims to manage risk and encourage the sharing of data by healthcare providers by ensuring they have control over how the information they produce is aggregated and used.

This proposed model is preliminary work in this area and future work could involve prototype implementations of an Information Accountability service for use in this decentralised model, verification of such a model using health data, further investigations into the challenges of implementing this approach at scale and user testing to verify the usefulness and acceptability of the model. Additionally, the use of this model for the purposes of providing opportunities for research and Health Big Data analytics on aggregated data sets could be explored.

In the next chapter, I conclude the thesis with a summary of the work, contributions, limitations, and future directions for the project.

8 Conclusions and Future Work

In this chapter, I conclude with a summary of the work and contributions of the thesis, identify the limitations of the research, and present some future directions for information accountability research in the context of eHealth.

8.1 Thesis Summary

In this thesis, the need to provide an appropriate balance between patient privacy requirements and the information access needs of HCPs in order for eHealth systems to succeed has been discussed. Through the use of information accountability and the proposed Information Accountability Framework protocols, such a balance can be realised.

The use of IA protocols provides mechanisms to ensure transparency and accountability of data use. In an AeH system, patients are aware of when, how, and why their information is accessed and used, while medical professionals are able to access the information they need to provide care to their patients and make informed decisions. As a result, AeH systems create an environment where health information is available to the right person at the right time without rigid barriers, whilst empowering patients with control over the use of their information.

I have defined an architecture for an Accountable-eHealth system, built and evaluated a prototype system, defined the security and usability requirements of AeH systems, and performed a user study with the prototype using standard usability testing protocols. I then extended the IAF model to address identified gaps, implemented the protocols into two existing EHR systems, and performed a pilot study using one of the implementations with HCPs in collaboration with researchers in Brazil. I found that AeH systems are a promising solution that augments existing security measures in eHealth systems with accountability to help balance the needs of patients and HCPs, and enable a means of reaping the full benefits from a shared eHealth record.

8.2 Contributions

This thesis makes a number of contributions to the body of knowledge around the application and implementation of IA in eHealth systems and the creation of usable and useful Accountable-eHealth systems. These contributions included the following:

- An architecture was proposed and the requirements for the functionality, security, and usability of IAF systems when implementing the protocols to produce AeH system were identified and validated through threat modelling, case scenarios, and a user study

- An extended model of the IAF allowing delegation of access was proposed, and the security and privacy requirements of the accountability mechanisms were presented to address gaps in the initial model

- The requirements for implementing the protocols into existing EHR systems were determined. These were explored and validated through two case studies that clearly demonstrated that it is possible to modify existing systems to support the IAF protocols

- An approach to applying the IAF model to decentralised systems was proposed

Overall, this work demonstrates that the creation of Accountable-eHealth systems is possible and presented how they can be implemented. Greater adoption of information accountability mechanisms in eHealth should lead to better delivery of healthcare services for the general public and the improved usefulness of shared eHealth record systems.

8.3 Limitations and Future Directions

In exploring the implementation of AeH systems, this thesis has provided the basis for future implementation of IA in real-world systems. However, there were several limitations of the work and it provides fertile ground for future research into Accountable-eHealth systems which I discuss in this section.

In Chapter 4, I performed a user study using standard usability testing protocols to evaluate the prototype system. This was performed with participants who filled the patient role in the system. In future, AeH systems could be further evaluated and the usability assessed through follow-up usability and qualitative studies with more diverse user types. These could include HCPs of different types, those fitting the role of administrator or HA, and those who may be delegated access in an EHR system such as carers in order to assess the expanded prototype presented in Chapter 5.

Likewise, the prototype system was evaluated for performance and scalability through small benchmarks due to limitations around being able to simulate a large scale eHealth system at this time. It would be a useful future direction to fully evaluate the scalability of AeH systems.

In Chapter 6, I explored implementing the IAF protocols into two existing EHR systems. An initial pilot study on the views of healthcare professionals was conducted using one of these implementations. I was not able to evaluate the implementation against actual health data and use cases. Future research could include making use of the implementation in systems such as FluxMED to further validate and investigate the use of the IAF and AeH systems. This could involve the use of a "shadow" implementation where the IAF logs what actions it would have taken in a given situation without initially changing the behaviour of the system for HCPs using the system. This would let us evaluate the IAF against actual user traffic in a non-invasive manner. It is also important to evaluate ways to make the creation of the default policies and rules for misuse scalable. It would be useful to explore creating implementations that use data such as how many times a policy needs to be overridden and in which situations that occurs to suggest improvements to rule sets.

Chapter 7 proposed making use of a modified IAF model for addressing the privacy concerns of combining data through a consent based approach. In the model, patients are able to opt-in to health trials and decide how and when their data can be shared with or combined with other databases as part of a study or for other use cases, while maintaining accountability and transparency. Additionally, the model aims to manage risk and encourage the sharing of data by healthcare providers by ensuring they have control over how the information they produce is aggregated and used. I did not evaluate an implementation of this model, and a possible future direction in the area of applying the IAF to Big Data Analytics and other decentralised use cases could involve implementation and user studies into the usefulness and acceptability of this approach.

Overall, a major future direction is to explore and evaluate implementing the IAF protocols in a real-world eHealth environment. This will require collaboration with people at many different levels of a health system.

Bibliography

ABC News (2016). Adelaide Crows coach killing: Health workers caught 'snooping' into files of Cy Walsh. Available: `http://www.abc.net.au/news/2016-02-23/health-workers-snooping-into-files-of-accused-crows-coach-killer/7194008`.

Adams, A. and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12):40–46.

Al-Fedaghi, S. S. (2007). Beyond purpose-based privacy access control. In *Proceedings of the Eighteenth Conference on Australasian Database - Volume 63*, ADC '07, pages 23–32, Darlinghurst, Australia. Australian Computer Society, Inc., Australian Computer Society, Inc.

Aldeco-Pérez, R. and Moreau, L. (2008). Provenance-based auditing of private data use. In *Proceedings of the 2008 International Conference on Visions of Computer Science: BCS International Academic Conference*, VoCS'08, pages 141–152, Swinton, UK. British Computer Society.

Alhaqbani, B. S. and Fidge, C. J. (2007). Access control requirements for processing electronic health records. *Business Process Management Workshops*, 4928:371–382.

Andreu-Perez, J., Poon, C. C., Merrifield, R. D., Wong, S. T., and Yang, G.-Z. (2015). Big data for health. *IEEE Journal of Biomedical and Health Informatics*, 19(4):1193–1208.

Appari, A. and Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, 6(4):279–314.

Appari, A., Johnson, M. E., and Anthony, D. L. (2013). Meaningful use of electronic health record systems and process quality of care: Evidence from a panel data analysis of us acute-care hospitals. *Health Services Research*, 48(2pt1):354–375.

Attorney-General's Department (2015). Serious data breach notification. Retrieved from `https://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx`.

Barka, E. and Sandhu, R. (2000). Framework for role-based delegation models. In *Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference*, pages 168–176, New Orleans, LA. IEEE.

Basin, D., Schaller, P., and Schlèapfer, M. (2011). *Applied Information Security: A Hands-on Approach*. Springer.

Batista, P., Grunwell, D., Sahama, T., and Campos, S. (2015). Medical Data Access Accountability in EHR Systems, A Practical Perspective. In *X-Meeting 2015 - 11th International Conference of the AB3C + Brazilian Symposium of Bioinformatics*, Sao Paulo, Brazil.

BBC News (2003). 'Dissident operation' uncovered. Available: `http://news.bbc.co.uk/1/low/northern_ireland/3038852.stm`.

Beautement, A., Sasse, M. A., and Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, NSPW '08, pages 47–58, New York, NY, USA. ACM.

Behrmann, G., David, A., and Larsen, K. (2004). A Tutorial on Uppaal. In Bernardo, M. and Corradini, F., editors, *Formal Methods for the Design of Real-Time Systems*, volume 3185 of *Lecture Notes in Computer Science*, pages 200–236. Springer Berlin Heidelberg.

Belden, J. L., Grayson, R., and Barnes, J. (2009). Defining and testing EMR usability: Principles and proposed methods of EMR usability evaluation and rating. Technical report, Healthcare Information and Management Systems Society (HIMSS).

Blumenthal, D. and Tavenner, M. (2010). The "meaningful use" regulation for electronic health records. *New England Journal of Medicine*, 363(6):501–504.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, pages 104–121, San Jose, California, USA. IEEE.

Bramble, J. D., Galt, K. A., Siracuse, M. V., Abbott, A. A., Drincic, A., Paschal, K. A., and Fuji, K. T. (2010). The relationship between physician practice characteristics and physician adoption of electronic health records. *Health Care Management Review*, 35(1):55–64.

Brinkerhoff, D. W. (2004). Accountability and health systems: toward conceptual clarity and policy relevance. *Health Policy and Planning*, 19(6):371–379.

Buntin, M. B., Burke, M. F., Hoaglin, M. C., and Blumenthal, D. (2011). The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health Affairs*, 30(3):464–471.

Byun, J.-W., Bertino, E., and Li, N. (2005). Purpose based access control of complex data for privacy protection. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, SACMAT '05, pages 102–110, New York, NY, USA. ACM, ACM.

CBC News – British Columbia (2013a). B.C. privacy breach shows millions affected: Ministry notifying more than 38,000 people about shared data. Available: `http://www.cbc.ca/news/canada/british-columbia/b-c-privacy-breach-shows-millions-affected-1.1342374`.

CBC News – British Columbia (2013b). 'Serious deficencies' blamed for 3 B.C. health data breaches. Available: `http://www.cbc.ca/news/canada/british-columbia/serious-deficencies-blamed-for-3-b-c-health-data-breaches-1.1354618`.

Chen, K., Chang, Y.-C., and Wang, D.-W. (2010). Aspect-oriented design and implementation of adaptable access control for electronic medical records. *International Journal of Medical Informatics*, 79(3):181–203.

Classen, D. C. and Bates, D. W. (2011). Finding the meaning in meaningful use. *New England Journal of Medicine*, 365(9):855–858.

Cornwall, A. (2002). Electronic health records: an international perspective. *Health Issues*, 73:19–23.

Cottle, M., Hoover, W., Kanwal, S., Kohn, M., Strome, T., and Treister, N. (2013). Transforming health care through big data: Strategies for leveraging big data in the health care industry. *Institute for Health Technology Transformation.*

Cresswell, K. M., Worth, A., and Sheikh, A. (2010). Actor-network theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making*, 10(1):1.

Croll, P. R. (2011). Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling. *International Journal of Medical Informatics*, 80(2):e32–e38.

CURE International (2015). HospitalRun. Retrieved from `http://hospitalrun.io/`.

CURE International (2016). Requirements: Medical coding. Retrieved from `https://github.com/HospitalRun/hospitalrun-frontend/wiki/Requirements:-Medical-Coding/2a3aff46314fac31406292c884c98637183b03ad`.

Cysneiros, L. M. and Kushniruk, A. (2003). Bringing usability to the early stages of software development. In *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International*, pages 359–360, Monterey, California. IEEE.

Davidson, S. B., Khanna, S., Milo, T., Panigrahi, D., and Roy, S. (2011). Provenance views for module privacy. In *Proceedings of the Thirtieth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, PODS '11, pages 175–186, New York, NY, USA. ACM.

DB-Engines (2016). DB-Engines Ranking of Graph DBMS. Retrieved February 2016 from `http://db-engines.com/en/ranking/graph+dbms`.

Department of Health (2014). Personally Controlled Electronic Health Record Review Report. Available: `http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth`.

Eberle, W. and Holder, L. (2009). Insider threat detection using graph-based approaches. In *Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security*, CATCH '09, pages 237–241, Washington, DC, USA. IEEE Computer Society.

Faria-Campos, A. C., Hanke, L., Batista, P. H., Garcia, V., and Campos, S. (2014). FluxMED: An Adaptable and Extensible Electronic Health Record System. In Campos, S., editor, *Advances in Bioinformatics and Computational Biology*, volume 8826 of *Lecture Notes in Computer Science*, pages 33–40. Springer.

Faulkner, L. (2003). Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behavior Research Methods, Instruments, & Computers*, 35(3):379–383.

Feigenbaum, J., Hendler, J., Jaggard, A. D., Weitzner, D. J., and Wright, R. N. (2011a). Accountability and deterrence in online life. In *Proceedings of the 3rd International Web Science Conference*, WebSci '11, pages 7:1–7:7, Koblenz, Germany. ACM, ACM.

Feigenbaum, J., Jaggard, A. D., and Wright, R. N. (2011b). Towards a formal model of accountability. In *Proceedings of the 2011 Workshop on New Security Paradigms Workshop*, NSPW '11, pages 45–56, Marin County, California, USA. ACM, ACM.

Feigenbaum, J., Jaggard, A. D., Wright, R. N., and Xiao, H. (2012). Systematizing "accountability" in computer science. Technical Report YALEU/DCS/TR-1452, Yale University, New Haven CT.

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

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., and Costa-Pereira, A. (2006). How to break access control in a controlled manner. In *Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on Computer-Based Medical Systems*, pages 847–854, Salt Lake City, UT. IEEE.

Flechais, I., Mascolo, C., and Sasse, M. A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1(1):12–26.

Gajanayake, M. N. R. (2013). *Practical issues when designing an information accountability framework for eHealth systems.* PhD thesis, Queensland University of Technology.

Gajanayake, R., Iannella, R., Lane, W. B., and Sahama, T. R. (2012). Accountable-ehealth systems: The next step forward for privacy. In *Proceedings of the 1st Australian eHealth Informatics and Security Conference*, Novotel Perth Langley, Perth, WA. Edith Cowan University, Edith Cowan University.

Gajanayake, R., Iannella, R., and Sahama, T. R. (2011). Sharing with care: An information accountability perspective. *IEEE Internet Computing*, 15(4):31–38.

Gajanayake, R., Sahama, T. R., Iannella, R., and Lane, B. (2013a). Designing an information accountability framework for ehealth. *e-Health Technical Committee Newsletter*, 2(2).

Gajanayake, R., Sahama, T. R., Lane, B., and Grunwell, D. (2013b). Designing an information accountability framework for ehealth. In *IEEE Healthcom 2013 15th International Conference on E-Health Networking, Application & Services*, Instituto Superior de Ciências Sociais e Políticas – Technical University of Lisbon, Lisbon, Portugal.

Garfinkel, S. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable*. PhD thesis, Massachusetts Institute of Technology.

Garfinkel, S. and Spafford, G. (1996). *Practical UNIX and Internet Security*. O'Reilly.

Garrety, K. and van Teeseling, I. (2012). E-Health: are we ready for this brave new world? In *ABC – The Drum*. Available: `http://www.abc.net.au/unleashed/4081982.html`.

Goldberg, L., Lide, B., Lowry, S., Massett, H. A., O'Connell, T., Preece, J., Quesenbery, W., and Shneiderman, B. (2011). Usability and accessibility in consumer health informatics: Current trends and future challenges. *American Journal of Preventive Medicine*, 40(5):S187–S197.

Gray, B. H., Bowden, T., Johansen, I., and Koch, S. (2011). Electronic health records: an international perspective on "meaningful use". *Issue brief (Commonwealth Fund)*, 28:1–18.

Grunwell, D., Batista, P., Campos, S., and Sahama, T. (2015a). Managing and Sharing Health Data through Information Accountability Protocols. In *Proceedings of the 17th International Conference on E-health Networking, Application & Services*, Boston, USA. IEEE, IEEE.

Grunwell, D., Gajanayake, R., and Sahama, T. (2014). Demonstrating Accountable-eHealth Systems. In *Proceedings of IEEE International Conference on Communications 2014*, pages 4258–4263, Sydney, NSW, Australia. IEEE, IEEE.

Grunwell, D., Gajanayake, R., and Sahama, T. (2015b). The security and privacy of usage policies and provenance logs in an Information Accountability Framework. In Maeder, A. and Warren, J., editors, *Proceedings of the Eighth Australasian Workshop on Health Informatics and Knowledge Management*, pages 33–40, Sydney, Australia. Australian Computer Society.

Grunwell, D. and Sahama, T. (2015a). Information Accountability and Health Big Data Analytics: A Consent-Based Model. In *Proceedings of the 17th International Conference on E-health Networking, Application & Services*, Boston, USA. IEEE, IEEE.

Grunwell, D. and Sahama, T. (2015b). The design and implementation of an Information Accountability Framework for eHealth systems. In *17th International Conference on E-health Networking, Application & Services*, Boston, USA. IEEE.

Grunwell, D. and Sahama, T. (2016). Delegation of access in an Information Accountability Framework for eHealth. In *Proceedings of the 9th Australasian Workshop on Health Informatics and Knowledge Management*, Canberra, A.C.T. ACM.

Grunwell, D. and Sahama, T. R. (2014). Designing and implementing usable and useful Accountable-eHealth systems. In *IEEE Healthcom 2014 16th International Conference on E-Health Networking, Application & Services*, Natal, Brazil. IEEE.

Haeberlen, A., Kouznetsov, P., and Druschel, P. (2007). PeerReview: Practical Accountability for Distributed Systems. *SIGOPS Oper. Syst. Rev.*, 41(6):175–188.

Hasan, R., Sion, R., and Winslett, M. (2007). Introducing secure provenance: Problems and challenges. In *Proceedings of the 2007 ACM Workshop on Storage Security and Survivability*, StorageSS '07, pages 13–18, New York, NY, USA. ACM.

Health Identifiers Act 2010 (Clth). Retrieved from `http://www.comlaw.gov.au/Details/C2010C00440`.

Hill, J. W. and Powell, P. (2009). The national healthcare crisis: Is eHealth a key solution? *Business Horizons*, 52(3):265–277.

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

HL7 International (2014a). Health Level Seven International. Retrieved from `http://www.hl7.org/`.

HL7 International (2014b). Provenance - FHIR v0.0.82. Retrieved from `http://www.hl7.org/implement/standards/fhir/provenance.html`.

HL7 International (2014c). SecurityEvent - FHIR v0.0.82. Retrieved from `http://www.hl7.org/implement/standards/fhir/securityevent.html`.

Holt, J. E. (2006). Logcrypt: Forward security and public verification for secure audit logs. In *Proceedings of the 2006 Australasian Workshops on Grid Computing and e-Research - Volume 54*, ACSW Frontiers '06, pages 203–211, Darlinghurst, Australia, Australia. Australian Computer Society, Inc.

Hooper, R. (2012). Health trust fined over data breach. In *The Independent*.

Hu, V. C., Kuhn, D. R., and Ferraiolo, D. F. (2015). Attribute-Based Access Control. *Computer*, 48(2):85–88.

International Organization for Standardization (ISO) (2014). ISO/IEC 27000 - Information technology – Security techniques – Information security management systems – Overview and vocabulary.

ISO 9241-11:1998 (1998). Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability. International Organization for Standardization.

Jagadeesan, R., Jeffrey, A., Pitcher, C., and Riely, J. (2009). Towards a theory of accountability and audit. In Backes, M. and Ning, P., editors, *Computer Security – ESORICS 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 152–167. Springer Berlin Heidelberg.

Jaspers, M. W., Steen, T., van Den Bos, C., and Geenen, M. (2004). The think aloud method: a guide to user interface design. *International Journal of Medical Informatics*, 73(11):781–795.

Jha, A. K. (2010). Meaningful use of electronic health records: The road ahead. *JAMA: The Journal of the American Medical Association*, 304(15):1709–1710.

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., Shields, A., Rosenbaum, S., and Blumenthal, D. (2009). Use of electronic health records in us hospitals. *New England Journal of Medicine*, 360(16):1628–1638.

Jin, J., Ahn, G.-J., Hu, H., Covington, M. J., and Zhang, X. (2011). Patient-centric authorization framework for electronic healthcare services. *Computers & Security*, 30(2):116–127.

Jolly, R. (2011). The e health revolution—easier said than done. Retrieved 5 May 2013, from `http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1112/12rp03`.

Kagal, L. (2014). Designing for accountability. In *2nd International Workshop on Accountability: Science, Technology and Policy*, Cambridge, MA USA.

Kahn, S. and Sheshadri, V. (2008). Medical record privacy and security in a digital environment. *IT professional*, 10(2):46–52.

Kandias, M., Virvilis, N., and Gritzalis, D. (2011). The insider threat in cloud computing. In *6th International Workshop on Critical Information Infrastructures Security*, pages 93–103, Lucerne, Switzerland. Springer.

Karsh, B.-T., Weinger, M. B., Abbott, P. A., and Wears, R. L. (2010). Health information technology: fallacies and sober realities. *Journal of the American Medical Informatics Association*, 17(6):617–623.

Keil, M., Beranek, P. M., and Konsynski, B. R. (1995). Usefulness and ease of use: field study evidence regarding task considerations. *Decision Support Systems*, 13(1):75–91.

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

Kierkegaard, P. (2012). Medical data breaches: Notification delayed is notification denied. *Computer Law & Security Review*, 28(2):163–183.

King, J. and Williams, L. (2014). Log your crud: Design principles for software logging mechanisms. In *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*, HotSoS '14, pages 5:1–5:10, New York, NY, USA. ACM, ACM.

King, J. T., Smith, B., and Williams, L. (2012). Modifying without a trace: General audit guidelines are inadequate for open-source electronic health record audit mechanisms. In *Proceedings of the 2Nd ACM SIGHIT International Health Informatics Symposium*, IHI '12, pages 305–314, New York, NY, USA. ACM.

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., and Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. In *2011 IEEE World Congress on Services*, pages 584–588, Washington, DC. IEEE.

Kuo, M.-H., Sahama, T., Kushniruk, A. W., Borycki, E. M., and Grunwell, D. K. (2014). Health big data analytics: Current perspectives, challenges and potential solutions. *International Journal of Big Data Intelligence (IJBDI)*, 1(1/2):114–126.

Kushniruk, A. W., Triola, M. M., Borycki, E. M., Stein, B., and Kannry, J. L. (2005). Technology induced error and usability: the relationship between usability problems and prescription errors when using a handheld application. *International Journal of Medical Informatics*, 74(7):519–526.

Kwankam, S. Y. (2004). What e-health can offer. *Bulletin of the World Health Organization*, 82(10):800–802.

Lana-Peixoto, M. A., Talim, L. E., Faria-Campos, A. C., Campos, S. V., Rocha, C. F., Hanke, L. A., Talim, N., Batista, P. H., Araujo, C. R., and Kleinpaul, R. (2011). Nmo-dbr: the brazilian neuromyelitis optica database system. *Arquivos de neuro-psiquiatria*, 69(4):687–692.

Lang, M. (2011). Reconciling usability and security: Interaction design guidance and practices for on-line user authentication. In Pokorny, J., Repa, V., Richta, K., Wojtkowski, W., Linger, H., Barry, C., and Lang, M., editors, *Information Systems Development*, pages 397–416. Springer.

Lehnbom, E. C., McLachlan, A., and Jo-anne, E. B. (2012). A qualitative study of australians' opinions about personally controlled electronic health records. In *Health Informatics: Building a Healthcare Future Through Trusted Information; Selected Papers from the 20th Australian National Health Informatics Conference (HIC 2012).*, Amsterdam. IOS Press Inc.

Li, M., Yu, S., Zheng, Y., Ren, K., and Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1):131–143.

Liaw, S.-T. and Hannan, T. (2010). Can we trust the PCEHR not to leak? *Aust Fam Physician*, 39:809–810.

Lieberman, D. (2012). Network Exposure and Healthcare Privacy Breaches. Retrieved from http://www.infosecisland.com/blogview/22099-Network-Exposure-and-Healthcare-Privacy-Breaches.html.

Locust (2016). Locust - a modern load testing framework. Retrieved from http://locust.io/.

Macefield, R. (2009). How to specify the participant group size for usability studies: a practitioner's guide. *Journal of Usability Studies*, 5(1):34–45.

Marcos, C., González-Ferrer, A., Peleg, M., and Cavero, C. (2015). Solving the interoperability challenge of a distributed complex patient guidance system: A data integrator based on HL7's Virtual Medical Record standard. *Journal of the American Medical Informatics Association*, 22(3):587–599.

McCann, E. (2013a). Advocate Health slapped with lawsuit after massive data breach. In *Healthcare IT News*.

McCann, E. (2013b). Bon Secours reports EHR data breach. In *Healthcare IT News*.

McCann, E. (2013c). New York hospital waits 15 months to announce HIPAA breach, notify patients. In *Healthcare IT News*.

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, 47(7):25–28.

Merkow, M. S. and Breithaupt, J. (2014). *Information Security: Principles and Practices*. Pearson Education.

Michener, B. (2014). Cayley: graphs in Go. Retrieved from http://google-opensource.blogspot.com.au/2014/06/cayley-graphs-in-go.html.

Microsoft (2005a). Applying STRIDE. Retrieved from https://msdn.microsoft.com/en-us/library/ee798544(v=cs.20).aspx.

Microsoft (2005b). The STRIDE Threat Model. Retrieved from https://msdn.microsoft.com/library/ms954176.aspx.

Microsoft (2014). Microsoft Threat Modeling Tool 2014. Retrieved from https://www.microsoft.com/en-au/download/details.aspx?id=42518.

Microsoft (2016). SDL Threat Modeling Tool. Retrieved from https://www.microsoft.com/en-au/download/details.aspx?id=42518.

Miles, S., Groth, P., Munroe, S., Jiang, S., Assandri, T., and Moreau, L. (2008). Extracting causal graphs from an open provenance data model. *Concurrency and Computation: Practice and Experience*, 20(5):577–586.

Naqvi, S., Dallons, G., Michot, A., and Ponsard, C. (2010). Assuring privacy of medical records in an open collaborative environment - a case study of Walloon region's eHealth platform. In Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., and Zhang, G., editors, *Privacy and Identity Management for Life*, volume 320 of *IFIP Advances in Information and Communication Technology*, pages 146–159. Springer Berlin Heidelberg.

National Institute of Standards and Technology (NIST) (2013). Usability. Retrieved from http://www.nist.gov/healthcare/usability/index.cfm.

Neo Technology (2016). Neo4j: The World's Leading Graph Database. Retrieved from http://neo4j.com/.

Neubauer, T. and Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics*, 80(3):190–204.

Nginx, Inc. (2016). nginx. Retrieved from http://nginx.org/en/.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., and Trombeta, A. (2010). Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 13(3):24.

OAIC (2014). Data breach notification — A guide to handling personal information security breaches. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

ODRL Initiative (2012). ODRL V2.0 - Core Model. Retrieved from http://www.w3.org/community/odrl/two/model/.

Oh, H., Rizo, C., Enkin, M., and Jadad, A. (2005). What is eHealth (3): A systematic review of published definitions. *Journal of Medical Internet Research*, 7(1):e1.

OpenEMR (2015). OpenEMR Project. Retrieved from http://www.open-emr.org/.

OpenEMR Project Wiki (2012). PhpGacl. Retrieved from http://www.open-emr.org/wiki/index.php?title=PhpGacl&oldid=12899.

OpenEMR Project Wiki (2013). Access Controls Listing. Retrieved from http://www.open-emr.org/wiki/index.php?title=Access_Controls_Listing&oldid=14981.

OpenEMR Project Wiki (2014). OpenEMR Features. Retrieved from http://open-emr.org/wiki/index.php?title=OpenEMR_Features&oldid=18739.

OpenMRS Inc. (2011). Access Control in OpenMRS. Retrieved from https://wiki.openmrs.org/pages/viewpage.action?pageId=20381784.

OpenMRS Inc. (2015a). OpenMRS. Retrieved from http://openmrs.org/.

OpenMRS Inc. (2015b). OpenMRS Atlas. Retrieved from https://atlas.openmrs.org/.

OpenMRS Inc. (2015c). Patient Portal Module - Personal Cancer Toolkit Project Revamp. Retrieved from https://wiki.openmrs.org/pages/viewpage.action?pageId=79665551.

Oracle Corporation (2016). MySQL. Retrieved from http://www.mysql.com/.

OWASP (2015). Threat Risk Modeling. Retrieved from https://www.owasp.org/index.php?title=Threat_Risk_Modeling&oldid=191011.

Pagliari, C., Sloan, D., Gregor, P., Sullivan, F., Detmer, D., Kahan, J. P., Oortwijn, W., and MacGillivray, S. (2005). What is eHealth (4): A scoping exercise to map the field. *Journal of Medical Internet Research*, 7(1):e9.

Parks, R., Chu, C.-H., and Xu, H. (2011). Healthcare information privacy research: Iusses, gaps and what next? In *AMCIS 2011 Proceedings - All Submissions*, Detroit, Michigan, USA.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77.

Personally Controlled Electronic Health Records Act 2012 (Clth). Retrieved from http://www.comlaw.gov.au/Series/C2012A00063.

Privacy Act 1988 (Clth). Retrieved from http://www.comlaw.gov.au/Details/C2013C00231.

Privacy Rights Clearinghouse (2016). Chronology of Data Breaches. Retrieved January 2016 from https://www.privacyrights.org/data-breach.

Rahim, F. A., Ismail, Z., and Samy, G. N. (2013). Information privacy concerns in electronic healthcare records: A systematic literature review. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pages 504–509, Kuala Lumpur. IEEE.

Richesson, R. L. and Chute, C. G. (2015). Health information technology data standards get down to business: maturation within domains and the emergence of interoperability. *Journal of the American Medical Informatics Association*, 22(3):492–494.

Rodrigues, J. J., de la Torre, I., Fernández, G., and López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of Medical Internet Research*, 15(8):e186.

Sasse, A. M. (2005). Usability and trust in information systems. In Mansell, R. and Collins, B. S., editors, *Trust and Crime in Information Societies*, pages 319–348. Edward Elgar.

Sasse, M., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122–131.

Schumacher, R. M. and Lowry, S. Z. (2010). NIST guide to the processes approach for improving the usability of electronic health records. *National Institute of Standards and Technology NISTIR 7741*.

Seneviratne, O. and Kagal, L. (2014). Enabling privacy through transparency. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, pages 121–128, Toronto, ON. IEEE.

Shahri, A. B. and Ismail, Z. (2012). A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. *Journal of Information Security*, 3(02):169.

Shyr, C., Kushniruk, A., and Wasserman, W. W. (2014). Usability study of clinical exome analysis software: top lessons learned and recommendations. *Journal of Biomedical Informatics*, 51:129–136.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. (2007). Password sharing: Implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 895–904, New York, NY, USA. ACM.

Sinha, A., Jia, L., England, P., and Lorch, J. R. (2014). Continuous tamper-proof logging using tpm 2.0. In Holz, T. and Ioannidis, S., editors, *Trust and Trustworthy Computing*, volume 8564 of *Lecture Notes in Computer Science*, pages 19–36. Springer International Publishing.

Snodgrass, R. T., Yao, S. S., and Collberg, C. (2004). Tamper detection in audit logs. In *Proceedings of the Thirtieth International Conference on Very Large Data Bases - Volume 30*, VLDB '04, pages 504–515, Toronto, Canada. VLDB Endowment.

Srur, B. L. and Drew, S. (2012). Challenges in designing a successful e-health system for Australia. In *2012 International Symposium on Information Technology in Medicine and Education (ITME)*, volume 1, pages 480–484, Hokodate, Hokkaido, Japan. IEEE.

Stamp, M. (2011). *Information Security: Principles and Practice.* John Wiley & Sons, Inc., 2nd edition.

The Apache Software Foundation (2016). The Apache Cassandra Project. Retrieved from `http://cassandra.apache.org/`.

The Go Authors (2016). The Go Programming Language. Retrieved from `https://golang.org/`.

The PHP Group (2016). PHP: Hypertext Preprocessor. Retrieved from `https://secure.php.net/`.

Tierney, W. M., Alpert, S. A., Byrket, A., Caine, K., Leventhal, J. C., Meslin, E. M., and Schwartz, P. H. (2015). Provider responses to patients controlling access to their electronic health records: A prospective cohort study in primary care. *Journal of General Internal Medicine*, 30(1):31–37.

Toscano, N. (2016). Health staff caught spying on Cy Walsh's medical records. Available: `http://www.smh.com.au/national/health-staff-caught-spying-on-cy-walshs-medical-records-20160223-gn1shx.html`.

Ulusoy, H., Colombo, P., Ferrari, E., Kantarcioglu, M., and Pattuk, E. (2015). GuardMR: Fine-grained Security Policy Enforcement for MapReduce Systems. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pages 285–296, New York, NY, USA. ACM.

Ulusoy, H., Kantarcioglu, M., Pattuk, E., and Hamlen, K. (2014). Vigiles: Fine-Grained Access Control for MapReduce Systems. In *2014 IEEE International Congress on Big Data*, pages 40–47, Anchorage, Alaska, USA. IEEE.

US Department of Health & Human Services (2015). Recruiting Usability Test Participants. Available: `https://www.usability.gov/how-to-and-tools/methods/recruiting-usability-test-participants.html`.

Van Bruggen, R. (2014). *Learning Neo4j*. Packt Publishing Ltd.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102. Cybercrime in the Digital Economy.

Weber, G. M., Mandl, K. D., and Kohane, I. S. (2014). Finding the Missing Link for Big Biomedical Data. *JAMA*, 311(24):2479–2480.

Weber-Jahnke, J. H. and Obry, C. (2012). Protecting privacy during peer-to-peer exchange of medical documents. *Information systems frontiers*, 14(1):87–104.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, 51(6):82–87.

Weitzner, D. J., Abelson, H., Berners-lee, T., Hanson, C., Hendler, J., Kagal, L., Mcguinness, D. L., Sussman, G. J., and Waterman, K. K. (2006). Transparent accountable data mining: New strategies for privacy protection. Technical Report MIT-CSAIL-TR-2006-007, MIT.

Westin, A. F. (1967). *Privacy and Freedom*. New York Atheneum.

Williams, P. A. (2011). Why Australia's e-health system will be a vulnerable national asset. In *Proceedings of the 2nd International Cyber Resilience Conference*, Perth Western Australia. Edith Cowan University.

Wood, W. A., Bennett, A. V., and Basch, E. (2015). Emerging uses of patient generated health data in clinical research. *Molecular Oncology*, 9(5):1018–1024. Clinical trials for development of personalized cancer medicine.

Yaffee, A. (2011). Financing the pulp to digital phenomenon. *Journal of Health & Biomedical Law*, 7(2):325–372.

Yang, N., Barringer, H., and Zhang, N. (2007). A purpose-based access control model. In *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*, pages 143–148, Manchester, UK. IEEE.

Yavuz, A. A., Ning, P., and Reiter, M. K. (2012a). BAF and FI-BAF: Efficient and Publicly Verifiable Cryptographic Schemes for Secure Logging in Resource-Constrained Systems. *ACM Trans. Inf. Syst. Secur.*, 15(2):9:1–9:28.

Yavuz, A. A., Ning, P., and Reiter, M. K. (2012b). Efficient, compromise resilient and append-only cryptographic schemes for secure audit logging. In Keromytis, A. D., editor, *Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 148–163. Springer Berlin Heidelberg.

Yee, K.-P. (2004). Aligning security and usability. *IEEE Security & Privacy*, 2(5):48–55.

Yee, K.-P. (2005). Guidelines and strategies for secure interaction design. *Security and Usability: Designing Secure Systems That People Can Use*, pages 247–273.

Zhang, J. and Walji, M. F. (2011). TURF: Toward a unified framework of EHR usability. *Journal of Biomedical Informatics*, 44(6):1056–1067.

Zurko, M. E. (2005). User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference*, pages 14–27, Tucson, AZ. IEEE.