Consent based privacy for eHealth systems

by

Ryan Habibi
B.Sc., Lakehead University, 2012

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Computer Science

© Ryan Habibi, 2018
University of Victoria

All rights reserved. This Thesis may not be reproduced in whole or in part, by
photocopying or other means, without the permission of the author.
Consent based privacy for eHealth systems

by

Ryan Habibi
B.Sc., Lakehead University, 2012

Supervisory Committee

Dr. D. Damian, Supervisor
(Department of Computer Science)

Dr. N. Ernst, Departmental Member
(Department of Computer Science)
ABSTRACT

Access to Personal Health Information (PHI) is a valuable part of the modern health care model. Timely access to relevant PHI assists care providers in making clinical decisions and ensure that patients receive the highest quality of care. PHI is highly sensitive and unauthorized disclosure of PHI has potential to lead to social, economic, or even physical harm to the patient. Traditional electronic health (eHealth) tools are designed for the needs of care providers and are insufficient for the needs of patients.

Our research goal is to investigate the requirements of electronic health care systems which place patient health and privacy above all other concerns.

Control of secure resources is a well established area of research in which many techniques such as cryptography, access control, authentication, and organizational policy can be combined to maintain the confidentiality and integrity of data. Access control is the dominant data owner facing privacy control. To better understand this domain we conducted a scoping literature review to rapidly map the key concepts underpinning patient facing access controls in eHealth systems. We present the analysis of that corpus as well as a set of identified requirements. Based on the identified requirements we developed Circle of Health based Access Control (CoHBAC), a patient centered access control model. We then performed a second scoping review to extend our research beyond just access controls, which are insufficient to provide reasonable privacy alone. The second review yielded a larger, more comprehensive, set of sixty five requirements for patient centered privacy systems. We refined CoHBAC into Privacy Centered Access Control (PCAC) to meet the needs of our second set of requirements. Using the conceptual model of accountability that emerged from the reviewed literature we present the identified requirements organized into the Patient Centered Privacy Framework. We applied our framework to the Canadian health care context to demonstrate its applicability.
# Contents

Supervisory Committee ........................................... ii

Abstract .................................................................. iii

Table of Contents .................................................. iv

List of Tables .......................................................... vii

List of Figures .......................................................... viii

Acknowledgements .................................................... ix

Dedication ................................................................. x

## 1 Introduction ......................................................... 1

1.0.1 Motivation ......................................................... 1

1.0.2 Research Approach .......................................... 5

1.0.3 Contributions .................................................. 6

1.0.4 Structure ......................................................... 7

## 2 Background and Related Work ....................... 9

2.1 eHealth Systems ................................................. 9

2.1.1 Circle of Care .................................................. 9

2.1.2 Personal Health Management ............................ 10

2.2 Data Privacy and Security ................................. 11

2.2.1 Security ......................................................... 11

2.2.2 Security Mechanisms ...................................... 13

2.2.3 Access Control ................................................. 14

2.2.4 AC in Health Care .......................................... 16
### Methodology

3.1 Grounded Theory Approach .............................................. 17
3.2 Scoping Literature Reviews ............................................. 18
3.3 Data Analysis ................................................................. 19
3.4 Conceptual Models ............................................................ 20

### Scoping Literature Reviews

4.1 Scoping Review on Advanced consumer facing Access Control Models ............................................. 22
   4.1.1 Stage 1. Identifying the research question ................. 22
   4.1.2 Stage 2. Identifying relevant sources ....................... 23
   4.1.3 Stage 3. Study selection ............................................. 23
   4.1.4 Stage 4. Charting the data ......................................... 25
   4.1.5 Stage 5. Collating, summarizing and reporting the results ... 28
   4.1.6 Synthesized Requirements ............................................ 34
   4.1.7 Circle of Health based Access Control ....................... 36

4.2 Scoping Review on Requirements for Patient Privacy ..................... 40
   4.2.1 Stage 1. Identifying the research question ................. 40
   4.2.2 Stage 2. Identifying relevant sources ....................... 40
   4.2.3 Stage 3. Study selection ............................................. 40
   4.2.4 Stage 4. Charting the data ......................................... 42
   4.2.5 Stage 5. Collating, summarizing and reporting the results ... 45
   4.2.6 Refinement of First Scoping Review Requirements .......... 57
   4.2.7 Synthesized Requirements ............................................ 61
   4.2.8 Privacy Centered Access Control ............................... 65

### Patient Centered Privacy Framework

5.1 Trusted Service Provider .................................................. 71
5.2 Storage ............................................................................. 72
5.3 Health Information Exchange .............................................. 73
   5.3.1 HIE Cryptography ..................................................... 73
   5.3.2 HIE Access Control ................................................... 74
   5.3.3 Guardians and Custodians ........................................... 76
   5.3.4 Information Accountability ......................................... 77
   5.3.5 Transparency ............................................................. 78
   5.3.6 Consent ................................................................. 78
5.4 Client .................................................. 80
  5.4.1 New Users ........................................ 80
  5.4.2 Access to Stored Information ..................... 83
  5.4.3 Mobile Clients and Sensors ......................... 85

6 Applying the Patient Centered Privacy Framework 86
  6.1 CanCare: A Privacy Centered eHealth System .......... 86
    6.1.1 Trusted Service Provider ......................... 87
    6.1.2 Storage ....................................... 87
    6.1.3 Health Information Exchange ...................... 88
    6.1.4 Clients ..................................... 95

7 Contributions and Implications, Limitations, and Future Work 98
  7.1 Contributions ..................................... 98
  7.2 Limitations ....................................... 99
  7.3 Future work ....................................... 101
  7.4 Conclusion ....................................... 102

A Scoping Review Search Queries 104
  A.1 First Review .................................... 104
    A.1.1 Compendex & Inspec ............................ 104
    A.1.2 Pubmed ...................................... 104
  A.2 Second Review ................................... 105
    A.2.1 Compendex & Inspec ............................ 105
    A.2.2 Pubmed ...................................... 105

B Scoping Review Search Results 106
  B.1 First Review Corpus ................................ 106
  B.2 Second Review Corpus .............................. 110

Bibliography 113
List of Tables

Table 4.1  Identified Requirements from First Scoping Review . . . . . . . 35
Table 4.2  Identified Requirements from Second Scoping Review . . . . . . 65

Table 5.1  Components of PCP Framework . . . . . . . . . . . . . . . . . . . 70

Table B.1  Literature Included in First Review Corpus . . . . . . . . . . . 110
Table B.2  Literature Included in Second Review Corpus . . . . . . . . . 112
List of Figures

Figure 3.1 Research Methodology Overview .......................... 17
Figure 3.2 Stages of Scoping Reviews ................................. 18
Figure 3.3 Sokoloski et al. Validation and Verification .......... 21

Figure 4.1 The Scoping Review Process for Review on Advanced Client-Centric AC Models ............................... 24
Figure 4.2 Access Control Policy Elements Concept Map .......... 27
Figure 4.3 Rath and Colin AC Requirements ............................ 29
Figure 4.4 Rath and Colin Usage Control Requirements .......... 30
Figure 4.5 Trojer Taxonomy of Access Control Requirements ...... 31
Figure 4.6 Barua Access Trees ........................................ 31
Figure 4.7 Picazo-Sanchez AC Lattice ................................. 32
Figure 4.8 Circle of Health Based Access Control Model .......... 36
Figure 4.9 The Scoping Review Process for Scoping Review on Requirements for Patient Privacy ............................. 41
Figure 4.10 Transparency, Storage, and Related Concepts from Figure 4.11 .................................................. 43
Figure 4.11 Access Control Patient Centered Privacy Concept Map .............................................................. 44
Figure 4.12 Privacy and Related Concepts from Figure 4.11 ...... 45
Figure 4.13 Schize Ideal EHR Structure ................................. 47
Figure 4.14 Spagnuelo & Lenzini Properties related to Transparency .............................................................. 53
Figure 4.15 Privacy Centered Access Control Model ................ 66

Figure 5.1 Simplified PCP Framework ................................. 69

Figure 6.1 CanCare implementation of PCAC ......................... 90
ACKNOWLEDGEMENTS

I would like to thank:

Dr. Price and Dr. Weber for all their support over the years,

Dr. Damian for believing in me and my work when I needed it most,

and my Grandma for supporting me in the low moments.
DEDICATION

Dedicated to Nom
Chapter 1

Introduction

1.0.1 Motivation

With the introduction of wearable and portable sensor technologies, consumers are able to generate more Personal Information (PI) than ever before. PI can be used by individuals to accomplish a variety of health, social, and economic goals. In the hands of health care providers, PI can reveal valuable contextual factors which may contribute to better health outcomes for patients. A patients’ Personal Health Information (PHI) encompasses all the PI that a patient generates about themselves as it applies to assisting them accomplish their health goals. This may include the information generated by care providers, legal guardians, data custodians, and trusted laypeople. For care providers, PHI such as accurate Electronic Medical Records (EMR) are a key component for providing accurate clinical assessment and care. PHI can be divided into two groups, clinical and non-clinical PHI. Clinical PHI is generated or approved by formal care providers and is relied on to provide insight into clinical decision making. Conversely, non-clinical PHI refers to any PI which in generated or edited by a layperson which can in some context assist care providers improve health outcomes. Some examples of non-clinical PHI include fitness data, dietary data, and contextual factors such as profession and living conditions. Non-clinical PHI can assist clinical decision making, however, it often requires organization or aggregation to be available to care providers in a useful format. Clinical PHI is generally considered to be more sensitive and for the remainder of this work we will address primarily the needs of clinical PHI. Non-clinical PHI should be treated as clinical PHI if it is relevant to care and thus any system which provides adequate protection for clinical PHI can support non-clinical as well.
Personal Health Information (PHI) is highly sensitive data about an individual’s life long health status and health related facts. It has been long established that PHI includes sensitive information, such as financial details, which may be used to harm the subject if exposed[1]. This makes PHI a desirable target for malicious hacking attacks. PHI is also at risk of unauthorized disclosure from insiders, both malicious and honest-but-curious. Despite the risks, PHI can be used to improve patient health outcomes. Clinical PHI is used by providers at the point of care and has been well established in their work flow by way of paper charts. Large amounts of collected PHI can also be data mined to uncover health trends and relevant contextual factors, often called “Population Health”[2]. Ultimately, patients themselves are the utmost authority on their privacy. The only way to share or access PHI in many jurisdictions is through their consent, although, traditional provider facing tools rarely prioritize patient consent.

Privacy of PHI is protected using privacy preserving security mechanisms. Access control (AC) is a fundamental building block of information security. Its main goal is to protect data from unauthorized read and write operations[3]. AC models are used in the design of secure systems. Of course, AC models are by no means the only mechanism needed to implement a secure information storage system. Other commonly required mechanisms include identification and authentication, data encryption, audit trails, etc. Platforms for sharing PHI are often called Health Information Exchanges (HIE). Most well documented HIEs have been provider facing with very little consumer involvement[4]. This leads to a disconnect between the needs of data owners and the design of privacy controls.

Some privacy mechanisms are implemented and maintained exclusively by service hosts. Data encryption and user authentication schemes are selected and enforced by the hosts and end users have little influence or control over their implementation. Training and education are required for selecting and enforcing appropriate security policies, so it is beneficial to have many security mechanisms managed exclusively by the host. AC policy and audit trails are examples of mechanisms which may be presented to users to empower them to manage some aspects of their data privacy. These mechanisms allows users to create a more tailored, or fine-grained, privacy policy. It is generally accepted that fine-grained AC is required for user controlled privacy of PHI.

The need for fine grain privacy controls in health care may, in part, derive from the universality of health care and health goals. This creates a large and varied
user population. Vulnerable populations, such as children, benefit from maintaining longitudinal PHI. They may be incapable of making informed decisions, which leads to a systemic need for guardians and data custodianship in the health care domain. Patients may visit several care providers per year. Patients may be co-morbid or have many parallel but related health interventions involving one or more groups of care providers. According to Price et al., the Circle of Care (CoC) is a system that is centered on a patient and contains the providers, information, and activities related to that patient’s care[5]. The CoC is more than just a business relationship. Patients have personal relationships with their care providers and establish a level of rapport, or trust. Trust relationships are constantly evolving and dynamic, and may change at any time based on the patient view of their evolving health context. Trust in eHealth systems may be considered a dynamic measure of a patient’s willingness to allow PHI to be recorded by a care provider or health organization. Patient facing privacy controls are one approach to improve patient trust in eHealth systems. Empowered patients can decide which care providers they trust with their information or what purposes it can be released. Patients may also desire to revoke access rights.

Patients benefit from sharing PHI with members of their CoC, even when those members may not be working together in the same care context. In order for patients to gain this benefit however, the privacy systems which guard it must be understandable and maintainable so that PHI can be shared with some degree of security. This is a complex and sparsely investigated problem. It is accepted that many factors, such as cognitive load[6], play a part in users’ ability to understand and actuate electronic tools. With a nearly universal population of users, the associated tools would need to be nearly universally understandable. Creating universal accessibility may not be feasible or even possible and little investigative work has been done to identify the requirements of patient facing systems to be understandable and maintainable. Furthermore, since the majority of existing tools are provider facing or designed in a provider centered way there is little historic evidence to assist in development of new, better, eHealth systems.

Problem Statement

PHI is sensitive and irreplaceable, once disclosed its confidentiality cannot be recovered. The health care domain has many stakeholders with many goals, however, two goals compete for precedence from a patient perspective: to achieve and maintain
the level of health the patient desires and to achieve and maintain the level of privacy the patient requires. eHealth systems are essential to meeting patient privacy goals, however, most are designed to be provider centered and don’t sufficiently involve patients. Since patient consent is the most important factor for disclosure of PHI we need privacy systems that allow efficient and accurate capture of consent directives from patients. We need a better understanding of patient centered health tools and the requirements, from a patient perspective, for how to make those tools understandable, maintainable, and sufficiently expressive.

There is significant overlap between this problem and similar problems in other domains in which users generate and store sensitive data, such as financial systems. However, we focus specifically on health care due to the ethical and social considerations. Care providers have an ethical responsibility not to harm their patients and how that relates to patient privacy, consent, and disclosure of PHI is still an open question which we seek to understand by linking the ethical obligations of care providers to the eHealth systems they use.

Research Goal and Questions

To address the above problem we have defined a research goal. To meet this research goal we have posed the following two questions.

We set the following as our research goal “To investigate the requirements of electronic health care systems which place patient health and privacy above all other concerns”. The design and development of eHealth systems is a resource intensive task and few systems are available for current analysis so we ask instead about the requirements of such systems.

Research Question 1:

To begin to address our research goal we must first better understand the domain. Health care is complex and constantly evolving. Our first research question is to better understand the assumptions underlying electronic health tools. “What is known in the current literature about AC models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility?”

Research Question 2:

Given that we were better able to understand the domain, AC, and AC’s role in providing consumer health we extended our scope to review what mechanisms extend beyond AC. Our second research question focuses on the patient centered require-
ments for such a system. “What are the requirements for access control and privacy controls in patient facing health systems with regards to creating comprehensible and maintainable privacy systems?”

1.0.2 Research Approach

Methodology

We attempted to answer our research questions through a grounded theory approach. Grounded theory is a systematic methodology which involves construction of theory through methodic gathering and analysis of data[7].

To better understand the key concepts underpinning the health care domain we performed two scoping reviews[8]. The first to determine the state of knowledge, or more specifically: ”What is known in the current literature about AC models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility”. This review revealed underlying assumptions about the domain as well as informed the creation of a patient centered AC model, Circle of Health based AC (CoHBAC), presented in section 4.1.7.

Access control was the key focus of the first review for its ability to collect consumer consent policy. The first scoping literature review indicated many needs for patient consent to be captured. However, there was little evidence of how these access controls were enforced or delivered to data owners. We formed our second research question to investigate the requirements of the broader privacy system: “What are the requirements for access control and privacy controls in patient health systems with regards to creating maintainable privacy systems” By asking what the requirements are of these systems we seek to develop concrete indicators of a health care systems ability to deliver patient privacy.

We identified a larger more comprehensive set of requirements from the second review. These requirements were used to further refine CoHBAC into Privacy Centered Access Control which is capable of meeting both old and new requirements. We then organized the requirements into a framework, the Patient Centered Privacy Framework, which maps the requirements for patient privacy to the stakeholders and services provided in an eHealth system. Our framework is based on the identified requirements as well as the conceptual model of privacy established by the literature reviews. To illustrate the applicability of the framework and validity of the identified requirements we designed a hypothetical eHealth system in the Canadian health care
context.

1.0.3 Contributions

In answering our research questions this work presents several contributions.

First, in investigating RQ1 we further the state of knowledge about patient facing eHealth tools. Our structured literature review provides a comprehensive basis of the available literature and current work on patient facing systems. On this basis a shared understanding of patient centered privacy can be established and used as our conceptual model for future patient facing eHealth tools.

From the first review we identified a set of ten requirements which guide the design of patient centered AC. This led to the development of our graph based patient centered AC mechanism, CoHBAC, which meets the identified requirements. This graph based AC model demonstrates an accountable consent focused approach in comparison to traditional provider centered tools.

To better understand the wider requirements for eHealth tools we continued investigating to answer RQ2. We performed a second scoping literature review. The results of this review further add to the shared basis of domain knowledge from which we can design patient centered tools and models. From this investigation we identified that although there is an acknowledged need for fine grain privacy systems for patient controlled PHI few complete schemes exists. Furthermore, though many security mechanisms, while some specific aspect or component of a mechanism are detailed, few complete schemes are presented and what is presented is not sufficient for reasonable expectations of privacy. We further contribute the sixty five (65) requirements for eHealth systems.

Applying the subset of the 65 identified requirements which apply to AC to our existing AC model, we developed a refinement of CoHBAC. We named this new, more generalized model Privacy Centered Access Control PCAC. PCAC meets all the requirements which bound CoHBAC as well as the refinements of those requirements identified through the second review. Furthermore, PCAC is designed so that it does not impede the non-AC requirements.

Our main contribution is the organization of the identified requirements in accordance with the conceptual model developed through the reviews. We named the result the Patient Centered Privacy (PCP) Framework. We recognized a core concept of accountability and organized the identified requirements into a framework around
that principle. The PCP Framework consists of a Trusted Service Provider, Health Information Exchange, Storage, and Clients. We demonstrate the applicability of this framework by way of the design of an eHealth system. Our illustrative system fulfills all the requirements of the PCP framework.

1.0.4 Structure

The remainder of this work is structured as follows.

In chapter 2 we broadly present the eHealth domain, the core stakeholders, and the needs of patients. We detail modern security mechanisms and terms and how they relate to eHealth. We go into further detail about Access Control and its central role to patients. The content in this chapter is necessary to understand the motivations of this research work.

Chapter 3 presents our approach to answer our research questions. We review grounded theory approach and scoping literature reviews as our mechanism for methodic gathering and analysis of data. We conclude by showing the relationship between conceptual models and requirements, both results of scoping literature reviews.

In Chapter 4 we present our scoping literature review in detail. We performed two successive reviews which are each presented including: research question being addressed, relevant sources, study selection criteria, charting of data, and reporting results. We produce intermediary results in the form of a preliminary set of requirements and graph based access control model which satisfies those requirements. We conclude with a larger, more covering, set of sixty five requirements identified by this work.

We present the Patient Centered Privacy (PCP) framework in chapter 5. This framework is an organization of the identified requirements following the conceptual model, also identified through the scoping review. This framework is designed to align the requirements with accountability from a patient perspective. In chapter 6 we present our vision of an eHealth system which is designed to meet the requirements of the PCP framework. We name this system CanCare and describe how it might meet the requirements in the Canadian legislative context.

We conclude with chapter 7, contributions and implications, limitations, and future work. This chapter reviews the contributions of this work and their implications for furthering the understanding of patient centered health care systems. We address
the limitations of our approach and suggest further areas of research which extend or refine our investigation.
Chapter 2

Background and Related Work

2.1 eHealth Systems

There are a wide variety of electronic health (eHealth) tools, services, and systems available to patients and providers. One of the most commonly available eHealth services is electronic health records (EHRs) storage and management. An EHR can be defined as “a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting”. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates and streamlines the clinician’s workflow. The EHR has the ability to generate a complete record of a clinical patient encounter - as well as supporting other care-related activities directly or indirectly via interface - including evidence-based decision support, quality management, and outcomes reporting.[9] We often consider EHRs as encapsulating all the clinical PHI, as opposed to contextual or personal health information, about a patient. Researchers have examined the benefits of EHRs including clinical and societal outcomes[10]. Clinical outcomes include improvements to quality of care and reduction in medical errors. Societal outcomes include being better able to conduct research and achieving improved population health.

2.1.1 Circle of Care

Many providers may contribute to a patient’s EHR. Price describes the Circle of Care (CoC) as a soft system that is centered on a patient and contains providers, information, and activities related to the patient’s care[5]. Relationships between
patients and the actors in their personal CoC are complex and constantly evolving around the current health care context. CoC’s can be quite extensive. In a US Medicare study, Pham found that patients managing multiple health concerns may see up to 16 physicians in a single year[11]. Furthermore, Price points out that providers in the CoC may not be limited to physicians, nurses, and other formal providers, but that this collection may also extend to include informal providers such as friends and family. We extend the CoC to encompass trusted laypeople who may assist a subject of care, or otherwise be involved with the patient’s management of their health concerns. We name this broader collection the Circle of Health (CoH). In addition to more comprehensively encompassing the actors who have a stake in an individual's contextual health care process, this extension also considers that many patients engage in their health care while not actively receiving treatment. Consider mobile fitness tracking and other mobile health tools which have the potential to allow individuals to proactively manage their health. Mobile devices can generate large amounts of health data, and as usage and adoption of these kinds of technology increases so will the desire to share and analyze this data for greater benefit. Connecting the professional and non-professional actors which make up a CoH is an important component of managing the long term health of the patient at the center of a CoH.

2.1.2 Personal Health Management

Use of smart devices and personal data tracking services allows individuals to generate large amounts of data about their health context. However, users possess the knowledge and skills to create meaningful metrics from their data. Users must agree to terms of service, often provided in difficult language, in order to track and aggregate data. While different services operate on different information ownership models, several important questions emerge from the transfer of PHI, such as: who can view the data? Who owns the data? To what extent can the data be erased? Many eHealth services maintain some level of ownership on the PHI stored with them. This allow the PHI to be analyzed, shared, or sold. Both the raw data and the inferences which can be made from its analysis are valuable. This can lead to a disconnect between users’ expectations of privacy and the potential consequences of subscribing to a service. PHI (including clinical, fitness, location, and demographic data) is sensitive. Publication of some or all of a patient’s data could have substantial social and
economic repercussions.

2.2 Data Privacy and Security

As personal health platforms mature, it is increasingly important for users to take control of their privacy as well as the data they protect. Kahn et al. describe principles for an ideal personal health record system as one that will require “information to be protected and private; that ownership lie solely with the consumer; that storage and use of the data be approved by the patients;”[12]. These three principals form a basis for patient centered policy. However, they are not sufficient to protect users from harm caused by misunderstanding and/or misuse of the system which adheres to these principles. Granting patients ownership and control in order to manage their data is not enough. Patients must have a sufficient level of contextual awareness and privacy control options must be presented in an accessible way. User centered design increases security by reducing human error when defining and reviewing privacy policy; this is accomplished by allowing users to define policy which closely resembles their mental model of their privacy needs. Having established the necessity for user centered design we present the remainder of this chapter to introduce security mechanisms which can be implemented in user centered systems and explain why Access Control (AC) systems are important from a patient perspective.

2.2.1 Security

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. The primary focus of information security is to balance confidentiality, integrity, and availability of data, often referred to the security triad, with some degree of efficiency and without hampering productivity.

Integrity

Integrity is defined as the “property of accuracy and completeness of data”[13]. In health care, complete and accurate data about ongoing treatments and treatment history facilitates better decision making by care providers. In the context of acute care, possible integrity concerns include: correct identification of patients and matching of patients to EMRs, accuracy of data recorded and stored by medical sensor devices
or providers, accuracy of data used at the point of care by providers and actuating devices. Failure to provide integral data can lead to poor clinical decision making and worse health outcomes.

The integrity of data needs to be maintained over the entirety of the data life cycle. PHI has a notably long life cycle. PHI which is generated in an acute care context has an immediate use in diagnosis and treatment but may also reveal patterns which inform later care. Similarly, integral data about a chronic illness may reveal trends if aggregated with similar personal or population data over time. Beyond acute care, PHI becomes a part of an individual's medical history and may impact future clinical decision making. PHI may also have use beyond the life time of the patient. If a patient discloses their PHI to a relative or descendant it can be used as part of that patient’s family history. Researchers may also desire access to populations of patients with similar conditions over long periods of time.

**Availability**

Availability is defined as the “property of being accessible and usable upon demand by an authorized entity”[13]. PHI has extremely high availability demands to be useful. Because a health emergency cannot always be predicted PHI must be available at all times. Furthermore, relevant PHI must be available for providers physically near their patients. This has been accomplished by paper records and many EHR systems are attempting to replicate that availability. Unfortunately, as the amount of PHI stored grows it can become more difficult to locate relevant data in a timely way. Clinical Decision Support (CDS) systems are one way which researchers are exploring to automatically filter large amounts of PHI and reference material to better inform and guide care providers.

**Confidentiality**

In information security, confidentiality “is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.”[13] Privacy is often discussed in terms of confidentiality. There are many proposed definitions for privacy. Generally, they all refer to the ability of users to express themselves selectively. Hue et al. use Westin's definition of privacy as representing the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent of information about them is communicated to others[14]. We will adopt
this definition as it has been used as the basis for the U.S. HIPAA, the European Data Protection Direction, the Data Protection Act of Japan, and other jurisdictions.

2.2.2 Security Mechanisms

There are many security mechanisms and policies which some combination of may be implemented into a specific privacy scheme. Many mechanisms are not user facing and end users have little or no control over their implementation. This includes internal security, such as anonymization of stored PHI or internal code auditing. From an end user’s perspective neither of these can be tested and must be assumed to be sufficient. These elements of a security scheme can be explained to users to help assure them and build trust. A privacy conscious user may refuse to use a system which cannot make such assurances.

Cryptography

Cryptographic schemes are an undeniably crucial part to secure message exchange but cannot be handled by end users. A lay person would not be able to select and implement an encryption scheme with any reasonable expectation of success. There are many public schemes which are resistant to attack, however, there is no guarantee that they may have undiscovered flaws which can be exploited. For this reason it is generally considered more secure to have encryption schemes only chosen, implemented, and maintained by trained individuals.

Authentication

Authentication protocols are another example of a security mechanism which cannot be controlled by end users. Authentication is often considered the most important protection for secure message transfer. Authentication protocols are used to establish identity and some measure of trust. If authentication protocols are too difficult, i.e. requiring too long or complicated a password, they may trade availability for confidentiality. Authentication is essential for ensuring that access to PHI can be granted in accordance to the patient’s wishes. There are some authentication schemes which empower end users. Certificate schemes and the like allow an authenticated user to express trust in other users. Even if end users are granted some measure of control there needs to exist a common criteria for trust which all users agree on.
Information Accountability

Information accountability schemes offer a way in which end users and developer can find common ground. Access logs which record all access, internal or external, can help deter misuse by associating an identity with each access request and allowing investigation in case of a breach. Audit logs must be maintained by the system authority but can be reviewed either automatically or by data owners. Automatic detection of questionable access can provide timely notification of malicious attacks or suspiciously misuse of legitimate access. Since data owners are the ultimate authority on their privacy they are also the most knowledgeable, in theory, to review access logs regarding their data. Information accountability is a powerful tool for controlling access a posteriori but does little to limit access in the first place.

2.2.3 Access Control

An access control (AC) model is a security mechanism that can be applied to limit access to sensitive resources. AC models allow users to define AC policy. AC policies are statements that define which states of a system are considered secure (allowed), and which other states of a system are considered insecure (forbidden). AC policies are known to be imperfect for complex application domains, such as health care. In practice, it is often unfeasible to define precise AC policies that take into account all possible health care scenarios and exactly distinguish between states that should be allowed and states that should be forbidden.

AC controls are the dominant user facing security control. They can allow data owners or administrators to define policy which can be tested at the time of access to determine to allow or deny. Because AC is most common and robust known tool for end users to protect their privacy it is the focus of our work. Generally, traditional access control mechanisms belong to four categories: Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-based Access Control (RBAC), and Attribute-based Access Control (ABAC).

MAC is control by a central authority which is empowered to determine what information can be accessed and by which subjects. The central authority acts as a security policy administrator. Information sensitivity is denoted by security labels which the policy administrator assigns. Historically and traditionally, MAC has been closely associated with multilevel security (MLS) and specialized military systems. The MAC model provides strong security guarantees as any user, even administrators,
are constrained by the defined policy. It is generally accepted that while MAC is strong for organizational security it is not flexible or convenient for execution[15].

DAC allows users to restrict access to data objects they own based on identity or membership to certain groups. Data owners may pass their rights to other users who may then pose a risk to the integrity and confidentiality of the data. For this reason DAC is traditionally used in environments with low levels of protection[15]. DAC has the advantage of collecting policy details directly from data owners. While this places the burden of maintenance on those owners there is clearly application in domains like health care where the end user is the authority on their own access policy.

Both MAC and DAC are flawed in that they require a significant investment to maintain, either by administrators or data owners respectively. RBAC is proposed under the motivation that a subject’s responsibility is more important than the subject itself.[15] Roles, which are groups of users, allow for levels of abstraction within the security model. This abstraction reduces the complexity of administration and improves maintainability by allowing for review of which users are assigned to which roles. RBAC has historically been implemented in many provider facing eHealth tools. This may be driven by the fundamental role difference between lay people and clinicians, as well as the training specializations of care providers.

In order to improve the flexibility of RBAC, it has been proposed to add attributes[16]. Attribute Based AC (ABAC) introduces a finer level of granularity in the defined policy. Furthermore, both actors and data can be described by the same set of attributes.

In addition to attributes, RBAC is usually implemented in combination with MAC or DAC to improve performance[17]. ABAC describes a large number of AC models, however, it has two significant flaws. First, it requires additional resources. The more complex the attribute scheme, or if users are allowed to define an arbitrarily level of complexity, the more work the cryptographic scheme needs to perform to ensure it reflects policy correctly. Secondly, and similarly, the added complexity is bad for maintaining such schemes over time as the complexity tends to grow.

In administrated systems, such as MAC, this difficulty can be somewhat mitigated with dedicated administrators. However, in DAC style systems the added complexity results in a steadily increasing risk of accidental disclosure. Furthermore, the lack of clarity creates a substantial concern about social engineering attacks against data owners. While AC is the first line of defence it is unable to defend against misuse of system resources by users who have been granted access[18].
2.2.4 AC in Health Care

There are many complex health scenarios where informed consent cannot be given by the patient including emergency situations where a patient is unresponsive or patients with disabilities or declining health that result in another individual being granted legal decision making power. The AC scheme must address the necessary trade-off between informational security (privacy) and patient safety in emergency situations. Thus the break-the-glass paradigm has been accepted to allow care providers to override access restrictions enforced by existing AC policies[19].

There is also a risk of care providers who may abuse their access rights to a patient’s PHI and potentially further disclose sensitive information. Although we do consider the possible malicious inside attacker we also consider an “honest but curious” attacker who accesses files without malicious intent or within their duties.

Our work considers patients to be the foremost authority for consent directives and views all other actors and stakeholders as requiring reasonable accountability for all their actions which relate to a patient’s PHI. In the next chapter we present our structured methodology to further add to our domain knowledge through scoping literature reviews. In chapter 4 we summarize and present the results of our scoping literature review which we combine with the above to form our basis of domain knowledge and conceptual model of health care.
Chapter 3

Methodology

In this chapter we will describe the research approach we use to investigate our research questions. We provide an overview of our methodology in figure 3.1. This methodology is based on a grounded theory approach to inductive reasoning.

3.1 Grounded Theory Approach

The health care domain is complex with many conflicting stakeholders. The needs of patients and providers can be drastically different depending on context, culture, and jurisdiction. While many authors detail specific areas of concern in health care few consider privacy systems as a whole. To better understand the key concepts underpinning patient privacy we take a grounded theory approach to map the requirements for patient centered privacy.

Grounded theory is a systematic methodology which involves construction of theory through methodic gathering and analysis of data[7]. Grounded theory is a methodology which operates inductively and often begins with a question or collection of data. Grounded theory can be modelled as having four stages of analysis: codes, concepts, categories, theory. As the data is reviewed, repeated ideas and
concepts become apparent and are tagged with codes. Codes can be grouped into concepts, and then into categories or themes. These categories become the basis for new theory. To collect the data to be analyzed we performed scoping literature review\[8\].

We considered this approach preferable to others such as directly interviewing primary users (patients, clinicians, system designers, etc.) as performing a literature review allows us to collect perspectives from a variety of legislative and social frameworks. Methodologies involving users typically have participants from the same country or social context. This could negatively influence our results away from our research goal to investigate the requirements of eHealth systems which place patient needs above all. In future work we discuss the value of modelling the social and legislative frameworks comparatively.

### 3.2 Scoping Literature Reviews

![Figure 3.2: Stages of Scoping Reviews](image)

A scoping study is a research method that aims to rapidly map the key concepts underpinning a research area, identify the main sources, and types of evidence available\[8\]. In contrast to ad-hoc literature reviews, scoping studies define explicit search plans that make them repeatable and scrutinizable. The search queries used in this work are provided in Appendix A. Scoping studies are performed in a five-stage process shown in figure 3.2:

1. Identifying the research question
2. Identifying relevant sources
3. Study selection
4. Charting the data
5. Collating, summarizing and reporting the results
Once a significant amount of data has been found from relevant sources it should be reduced to better fit the scope of the research question. The third stage, study selection, can further focus results through successive filtering steps applied to the identified literature. We applied three success filters to identified literature. First, we applied use of various controlled and uncontrolled vocabularies in our search queries. The vocabulary differs from source to source but relevant terms were selected to best fit the research question. The resultant corpus was subjected to a meta-data review. We examined each title and abstract and applied a series of inclusion/exclusion rules to determine which were on topic. Finally, we performed full text reviews and applied a final set of inclusion/exclusion criteria to produce the final corpus. The final set of included literature is presented in Appendix B.

3.3 Data Analysis

Grounded theory data analysis can be performed in four successive steps: codifying the corpus, grouping codes on similar content into concepts, identifying broad categories of similar concepts, generating theory from categories.

The identified literature was extensively coded in relation to the research question. Coding involves taking a small chunk of the text, line by line, and identifying key phrases which are marked and named. Another chunk of text is then taken and the steps repeated. This is called open, or initial, coding. Subsequent steps involve more theorizing and when coding is being done examples are being pulled out, examples of concepts together. Coders must consider how each concept can be related to a larger more inclusive concept. This involves the constant comparative method and it continues throughout the grounded theory process, right up through the development of complete theories.

Codes can be organized into concepts by charting the data. Charting describes a technique for synthesizing and interpreting qualitative data by sifting, grouping and sorting material according to key issues and themes[20]. We used the Institute for Human and Machine Cognitions (IHMC) Concept Map (CMap) tool for charting the selected literature. Each paper was reviewed according to key issues and themes discussed, which would give rise to new concepts or new concept relationships in the CMap.

By visualizing the concepts and relationships between them we are able to broadly group concepts into categories. Both concepts and categories are related to the re-
search question. Categories, in grounded theory, are used to generate theory. The final step of our review is using categories and concepts to define requirements which can be used in the development and design of privacy systems and address our research goal. By generating requirements from the analysis we seek to answer RQ2.

3.4 Conceptual Models

A conceptual model is a set of concepts which form a representation of a system and can be used to understand the subject the model represents. Conceptual models are often abstractions of things in the real world whether physical or social. A conceptual model’s primary objective is to convey the fundamental principles and basic functionality of the system which it represents. Also, a conceptual model must be developed in such a way as to provide an easily understood system interpretation for the models users. A conceptual model, when implemented properly, should satisfy four fundamental objectives[21].

- Enhance an individual’s understanding of the representative system
- Facilitate efficient conveyance of system details between stakeholders
- Provide a point of reference for system designers to extract system specifications
- Document the system for future reference and provide a means for collaboration

Conceptual models play an important part in the software development life cycle. Figure 3.3 from Sokoloski et al. shows the role of the conceptual model in typical development[22]. If the conceptual model is not fully developed it may lead to future problems or system shortcomings. These failures do occur and have been linked to; lack of user input, incomplete or unclear requirements, and changing requirements. In investigating RQ1 we will build up a conceptual model of the domain from the evidence in current literature alongside more formal requirements.

To conclude our methodology we will organize all identified requirements and conceptual model into a conceptual framework. In doing so we lend structure to our results which follows logically from investigation into the domain. Furthermore, the resultant framework can be used to further develop and verify both the conceptual model and the requirements. Our framework will be developed in accordance to the major recurring concepts and categories identified across both scoping literature reviews.
In section 4.1 we present the first literature review which is aimed at better understanding the domain. We synthesis the first set of requirements in section 4.1.7 and present our access control model which meets those requirements in section 4.1.8. We present the second literature review in section 4.2, presenting the more complete set of requirements in section 4.2.7. In chapter 5 we organize the identified requirements into a framework. And in chapter 6 we demonstrate the applicability of the framework by applying it in the Canadian health care context. We conclude with chapter 7 in which we review contributions, discuss limitations, and suggest future related work.
Chapter 4

Scoping Literature Reviews

Too better understand the domain and answer our research questions we performed a scoping literature review. In section 4.1 we address our first research question and develop a strong basis of knowledge. In section 4.2 we address the second research question including the formal definition of the requirements of patient centered systems.

4.1 Scoping Review on Advanced consumer facing Access Control Models

4.1.1 Stage 1. Identifying the research question

A scoping study is a research method that can be used to rapidly map the key concepts underpinning a research area, identify the main sources, and types of evidence available.[8] To better understand consumer health needs we identified the following research question for the initial scoping review:

“What is known in the current literature about AC models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility.”

Our focus was on access control as it is the dominant security mechanisms for gathering patient consent. To better understand how AC can impact patients we specifically investigated how effective these scheme were in the context they were developed. We also are concerned about the limitations of existing solutions as they may indicate in what ways user’s needs are not being met. We lastly consider the
comprehensibility of these models to determine how patients understand their tools and to what degree they can manage them.

4.1.2 Stage 2. Identifying relevant sources

There exists a large number of potentially relevant information sources both in Engineering and Health Informatics literature. Given the fact that newer publications in this area tend to be available in electronic databases, we restrict ourselves to searching electronic sources only. The following primary sources were selected:

- COMPENDEX (COMPuterized ENgineering inDEX); An electronic index of engineering literature covering a large number of journals, conferences and workshop proceedings from over 190 engineering disciplines.

- INSPEC; An electronic meta index covering a large number of scientific and technical literature sources.

- Pubmed; An electronic meta index for publications in the fields of medicine, nursing, dentistry, veterinary medicine, health care systems, and pre-clinical sciences.

Publications over a period of ten years from the time of the search were deemed relevant: 2004-2015. The review focused exclusively on publications written in English.

4.1.3 Stage 3. Study selection

Studies were selected according to three successive filtering steps. The results of are presented in figure 4.1.

The first selection step applies keyword queries on the meta data of publications indexed in the defined data sources. The meta data includes the publications title, its keywords, as well as its abstract. Controlled vocabularies are used when available for the keyword queries.

Inspec and Compendex provide controlled terms for “access control”, “health care”, “health” and “social networks”. In order to further focus the query results, several controlled terms were excluded. Moreover, we added uncontrolled keyword
searches for “patient”, “client”, or “consumer” in the meta-data (title, abstract, keyword) to establish a focus on health consumers. The full query is available in Appendix A. The query resulted in 124 unique publications from Compendex/Inspec.

The Pubmed indexing database has a controlled vocabulary of search terms called MeSH (Medical Subject Headings). The following MeSH terms were selected: “personal health records”, “consumer health information”, “social support”, “confidentiality”, and “computer security”. The full query is available in Appendix A. Pubmed produced 49 more unique publications.

The meta-data of each query result was reviewed according to the following inclusion/exclusion criteria:

- **[E1]** - Exclude if meta-data (title/abstract/keywords) does not express any focus on consumer-facing health informatics application. This may be expressed by mentioning a consumer-facing technology (such as PHR), a representative of such a technology (such as Google Health), the reference to consumers/patients as direct users of a system, or the use of terms that indicate a patient-facing
component of the IT solution (e.g., Telehealth).

- [E2] - Exclude if meta-data does not express any focus on patient driven AC or security models.
- [I3] Include otherwise

Of the 124 unique publications from Compendex/Inspec the meta data review excluded 85 papers. The meta data review on articles returned by Pubmed excluded 38 papers of the 49 returned. A total of 50 papers remained, from all sources, for the full text review.

Each of the remaining 39 papers from Compendex/Inspec and 11 papers from Pubmed had its full text reviewed and the following inclusion/exclusion criteria were applied, removing 29 papers from the result set:

- [I4] - Include if paper describes an AC model to the level of detail that allows the reader to formulate concrete AC policies, based on what is described in the paper.
- [I5] - Include if paper describes a formal model for reasoning / evaluating AC policies based on some notion of quality.
- [I6] - Include if paper describes user or domain requirements as a framework for future implementation of concrete AC policies.
- [E3] - Exclude otherwise.

The resultant 31 publications are considered the corpus of this review. We subjected the corpus to full text analysis. We present the complete list of included literature as Appendix B.

4.1.4 Stage 4. Charting the data

Charting [20] describes a technique for synthesizing and interpreting qualitative data by sifting, charting and sorting material according to key issues and themes. We used the Institute for Human and Machine Cognitions (IHMC) Concept Map (CMap) tool for charting the selected literature. Each paper was reviewed according to key issues and themes discussed, which would give rise to new concepts or new concept relationships in the CMap. Based on these concepts, high level categories were identified
and reported in the next stage. The concept map in figure 4.2 centres on AC policy elements and relates them back to the schemes reported in the corpus.

The concepts identified in figure 4.2 aided in the development of the requirements presented in section 4.1.6. To better understand the relationship between the concepts and the identified requirements in table 4.1 we present the following examples:

Trojer et al. reported the results of a questionnaire to German patients to understand their values and expectations of health services.[23] Trust relationships were reported to be considered the most important factor by respondents. Thus, trust based AC, also sometimes called reputation based AC, was added as a type of AC policy element in figure 4.2. This was further supported by [24] who present an AC scheme in which each user has a calculated reputation score. As user trust in providers was a repeated theme across much of the corpus this lead to the development of the seventh requirement: Differentiate CoC by trust criteria. (Patients may have multiple CoCs).

Healthcare is episodic and treatment follows a life cycle dictated by the nature of the illness and feedback or observations of the patient’s response to treatment. Sicuranza and Esposito proposed an AC scheme which which significantly adds a temporal extension that allows patients to provide time-limited consent directives.[25] This led to the addition of temporal AC as a type of AC policy element in figure 4.2 and eventually to the development of the eight requirement, to allow for ephemeral CoCs as well as for persistent ones. This was further indicated by the needs of emergency systems such as the one presented by Chen et al.[26] The requirement of ephemeral CoCs not only allows for temporal restrictions but also for the creation of contextual groupings which are granted access under other temporary states, such as a state of emergency. This demonstrates that not every concept maps to a unique requirement, however, all concepts are represented somehow in the requirements.
Figure 4.2: Access Control Policy Elements Concept Map
4.1.5 Stage 5. Collating, summarizing and reporting the results

The following section discusses the concepts that contributed to figure 4.2 and how they relate the literature in the corpus. We conclude this section by presenting the synthesized requirements and our Circle of Health Based AC model which is capable of meeting those requirements.

Health Care Domain

Several authors characterize requirements that should govern the design of AC mechanisms for patient-controlled PHI, referencing legal policy frameworks in different jurisdictions. Hue et al. [14] use Westins definition of privacy as representing: “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent of information about them is communicated to others” This definition has been used as the basis for the U.S. HIPAA, the European Data Protection Direction, the Data Protection Act of Japan, and other jurisdictions. Based on this definition Hue et al. suggest several requirements for patient-focused AC models.

A more detailed classification of requirements on AC policies has been presented by Rath and Colin [27] in figure 4.3. Their requirements were elicited in the context of a European PHR project and consider two viewpoints, the viewpoint of the data owner as well as the viewpoint of the data user. They also present a taxonomy on usage control requirements from data owner perspective in figure 4.4.

Similar sets of requirements have been captured by Rstad and Nytr [28] in the context of PHR systems and Sicuranza and Esposito [25] in the context of EHR systems that provide facilities for patient consent directives.

Carrin Seor et al. present a comprehensive systematic review of the AC models of existing PHR apps and services [29].

A large-scale empirical study on consumer requirements and factors influencing patient-centric AC model requirements has been published by Trojer et al. [23]. The study was carried out in the German context and utilized a questionnaire on 719 respondents, of which 513 complete answers were evaluated. The study accounts for different consumer demographics and different health care use cases. It differentiates the importance of factors influencing the design of AC models from a consumer perspective. Based on their answers, the patient population could be roughly divided into three consumer stereotypes, referred to as (1) the Responsible patient, (2) the
Balance-advocating patient and (3) the Privacy-sacrificing patient. Trust relationships were seen as the most important factor. Trojer et al. provide a taxonomy summarizing all access control factors that were named by respondents, shown in figure 4.5.

**Information types / sensitivity levels**

The collected literature captures a broad spectrum of consumer health applications, including: telemedicine services, personal health records, diagnostic apps, and health management apps. The PHI accessed and controlled in these systems is consequently also of heterogeneous character. Most articles discuss AC models pertaining to controlling access to PHI that is used as core information for clinical decision making. Few publications discuss contextual information, such as patient beliefs, priorities, personal living situation etc. Still, most AC models consider that there exists PHI at different levels of sensitivity and use a notion of sensitivity levels for policy definition and making access decisions[30]. Information access may be organized according to access trees where higher levels of clearance imply access to more sensitive information, as shown in figure 4.6.
Access Control Policy Elements

Role-based AC (the dominant AC model applied in many provider-facing EHRs) is commonly not seen as providing sufficient granularity for patient-controlled PHI. Most patient centered AC models provide at least a combination of role-based and identity-based policy statements. Ssembatyas AC model uses simple boolean predicates to specify AC policies that comprise roles as well as identities of information request makers[31].

The concept exists that an access tree can be generalized to that of an access lattice of PHI content that is not only sorted by sensitivity but also by concern categories. Figure 4.7 shows an example, taken from Picazo-Sanchez et al.[32]. Each node in the AC lattice has a security label that consists of a sensitivity level and one or several concern categories (generally referred to as compartments) in Computer Security. Protected resources (PHI elements) are attributed with these security labels. Actors who request access to these resources are given similar security labels (commonly referred to as clearances).

AC models that use fine-grained data compartments for protecting PHI has been presented by Hue et al.[14], Kandasamy and Papitha[33] and Qian et al.[34] The distribution and protection of these fine-grained data compartments can either be
organized based on a selective encryption scheme applied to a larger data set (such as a clinical summary in the HL7 Clinical Document Architecture) or it can be aligned with emerging fine-grained resource-centric interoperability standards, such as HL7 FIHR[35]. The latter approach is considered less complex and easier to implement and maintain.

Several consumer-focused AC models use purpose-based consent directives. In other words, consumers not only specify who should be allowed to access their PHI, but also for what purposes[36]. Purposes may be organized hierarchically in AND/OR-trees, where goals (purposes) are composed of conjunctions or alternatives of sub-goals.

Workflow-based AC models utilize a detailed model of the care process / workflow that requires the use of PHI. It recognizes that actors in the care workflow require
access to certain PHI only at particular steps in the process and seeks to limit access permissions to these particular steps. Leyla and MacCaull present a workflow-based AC model[37].

The fact that healthcare is episodic means that access to PHI often has a temporal character. Several researchers have suggested temporal extensions to traditional AC models. Sicuranza and Esposito propose a combination of RBAC, mandatory access control (multi-level) and a temporal extension that allows patients to provide time-limited consent directives.[25]

Purpose-based AC models can be generalized to the notion of context-based AC, where a declaration of purpose is one of many contextual factors that may be specified in AC policies. Other contextual factors may deal with temporal or spatial aspects of the access, or the use of specific devices or networks. Bhatti et al.[38] describe several examples, including the following which makes a clear case for this type of access: “physician d1 can access a record of type X of patient p1 when accessing from or near ABC hospital on the first Wednesday of the first month of every quarter between 9 and 5 pm” Yarmand et al. extend context-based AC by adding a notion of accounting for requester behaviour, e.g., modelling typical access patterns.[39] This AC model is referred to as “behaviour-based AC”.

Health care consumers may want to share PHI about themselves with health care professionals as well as informal caregivers (friends and family). Not all potential request makers may be known to the data owner. Ibraimi et al. propose an AC model that uses the concept of “reputation” to assist consumers with issuing consent
directives in these cases[40]. The reputation of an information requester is computed as an aggregate value based on the trust that other actors in the social network have in the requesting individual.

Research on privacy policies in social health network applications have shown that patients often tend to compromise their privacy for (perceived) short-term benefits and often do not understand the effect of their privacy controls.[41] Therefore, patient-generated privacy settings cannot solely be relied on for protecting patient privacy and mitigating security risks.

AC policies and consent directives may become complex and difficult to define/understand for data owners. Negative AC policy statements in combination with common defaults may be used to reduce this complexity. Rstad & Nytr propose the combination of a set of common policies defined for a patient (consumer) population with individualized personal policies that allow consumers to customize and extend the common policy defaults.[28]

Some AC models support protocols for “on the fly” consents solicited by health consumers, leveraging the fact that a large number of patients have smart phones and can respond to access requests with little delay.[42] Of course, in emergency situations, patients may not be able to provide consent themselves. An emergency contact group in the patients circle of care can perform this function on their behalf.[26]

A similar yet more generalized AC model for consent overrides has been proposed by Weber-Jahnke and Obry.[19]

Liang et al. explore the use of ad-hoc mobile spatial social networks for distributing and serving calls and PHI distribution in cases of consumer health emergencies.[43]

The ability to revoke consent directives is a requirement in many jurisdictions. From an abstract perspective, revocation can simply be seen as a modification of a previous consent directive, i.e., a rewriting of an AC policy statement. However, from an implementation point of view, access to PHI that has already been distributed may be difficult to revoke. Several researchers discuss revocation as an important aspect to be considered in the design of the implementation of an AC system. Common models rely on cryptographic approaches that use key management schemes where access keys are distributed rather than information content (and keys can be revoked).[33] Of course, such a key distribution scheme may cause a “key escrow” trust problem, where keys are held at a central entity that must be trusted by the health consumer to properly enforce their consent directives[44]. Shared key cryptographic schemes have been developed to avoid the need for such a trusted central entity such as those
proposed by Li et al.[44], Weber-Jahnke and Obry[19].

**Access Control in the Cloud**

Several researchers have concentrated their work on developing mechanisms for enforcing AC policies in a cloud-based environment, both trusted and semi or untrusted. Such enforcement mechanisms are often based on distributed cryptographic protocols, Bruce et al.[45], and distributed access tokens, Ge et al.[46].

**Human Factors**

Margheri et al. point out that many formalisms for defining AC policies are not user-friendly and impede human understanding[47]. They describe a formalism that facilitates human understanding yet has a formal mathematical basis and thus provides for machine-based interpretation. Tojer et al. present a framework for developing AC policies and AC policy authoring tools from an end-user (patient) perspective and with emphasis on usability testing[48]. Ruan proposes a visual approach to modelling AC policies based on the Unified Modelling Language (UML)[49].

**Verification and Validation of AC Policies**

There is an inherent trade-off between AC (which has the goal to limit access to PHI) and information flow effectiveness (which has the goal to provide PHI to all actors in health care who may require it). Sometimes this trade-off is referred to as information privacy vs. patient safety (health care effectiveness). Several authors have proposed methods for evaluating / determining the best balance between information protection and information flow effectiveness. Trojer et al. have presented an approach to formally represent properties related to information flow effectiveness and to use this model to validate patient centered AC policies for potential conflicts with health care goals[48].

**4.1.6 Synthesized Requirements**

Following from our analysis of the concepts and their relationships we identified 10 requirements for AC in patient centered eHealth systems. We present these requirements in table 4.1 grouped categorically based on our interpretation of the concept map in figure 4.2
<table>
<thead>
<tr>
<th>Data objects</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Differentiate data by sensitivity</td>
</tr>
<tr>
<td>2</td>
<td>Differentiate data by type or treatment (episodic) context</td>
</tr>
<tr>
<td>3</td>
<td>Maintain data provenance (origin, time of creation, time of last access)</td>
</tr>
<tr>
<td>4</td>
<td>Provide data compositionality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subjects</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Subjects may be individuals or entire organizations</td>
</tr>
<tr>
<td>6</td>
<td>Subjects may be allowed to contribute data or may only view data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Circle of Care</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Differentiate CoC by trust criteria. (Patients may have multiple CoCs)</td>
</tr>
<tr>
<td>8</td>
<td>Allow for ephemeral CoCs as well as for persistent ones.</td>
</tr>
<tr>
<td>9</td>
<td>Subjects are allowed to stay anonymous with respect to other subjects in the CoC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>The AC Model should be easy to use and comprehend from a patients perspective</td>
</tr>
</tbody>
</table>

Table 4.1: Identified Requirements from First Scoping Review
4.1.7 Circle of Health based Access Control

We developed the Circle of Health Based Access Control (CoHBAC) model in figure 4.8 to meet the ten requirements identified from the literature review.\(^1\)

The method is based on graphs and graph transformation systems[51]. CoHBAC is a generalizable patient centered privacy control paradigm and is intended to be extensible and flexible so that implementations can be adjusted as patients and health care professionals needs evolve. CoHBAC is unique in that user trust is incorporated into the design, empowering patients to make informed privacy decisions based on their personal health care context. To better match the patient’s mental model of their health care context, all privacy controls are implemented on groups of actors (referred to as circles) which relate directly to the patients’ health and wellness concerns. Users are able to conceptualize AC policy from their existing event based contexts and longitudinal concerns; this allows CoHBAC to better map changes in user context to policy creation or maintenance than traditional AC paradigms. All users in the CoHBAC model are actors. Two principal types of actors exist: patient or provider for a given context. At a high level this separates users by their role

---

\(^1\)This work was published in GRAMSec 2017[50]
as either professional health care providers or laypeople. The main distinction between providers and patients is that the latter have their own CoHs and information to maintain. This role division can be further decomposed at need. Although all laypeople in this model are patients, in any given user’s context only they are the subject of care with the other members of their CoH being friends, family, etc. The provider role is not restricted to refer to primary care providers such as physicians and nurses but extends to specialists as well. Organizations can also be represented as providers. Organizations such as care facilities, support groups, and health authorities can act as a single provider when appropriate. It follows from the trust based design that no individual or group processes the right to violate the privacy controls enacted by the patient. In essence, the patient always possesses final decision making power over their data.

**Satisfying Requirements**

In understanding the development and design of CoHBAC we refer back to the ten identified requirements from the literature review. The data objects, denoted as PHI in figure 4.8, can be described and constrained by a set of attributes. The specific attributes included are intended to be extended, or simplified, based on the specific eHealth implementation. [R1],[R2], and [R3] can be satisfied by including the appropriate attributes as modeled in figure 4.8. [R4] is met by including a self-referential contains relationship to data objects such that any data may be a collection that includes other data but allows for access controls to be implemented on any level of the data hierarchy. The patient (sometimes referred to as the subject of care or primary actor) may have any number circles by [R7]. Actors have no inherent identity constraints within the model though may explicitly be identified as a provider [R5] if they are qualified. Any actor can be made a member of a patient’s circle and in doing so is allowed to choose anonymity options within that context, by [R9], and can be given editing rights satisfying [R6]. As circles are constrained by the same set of attributes as data it is possible to meet [R8] by defining a set of attributes which indicate a time frame or explicit expiry for permissions. [R10] is more challenging to prove due to its dependence on interface and implementation however the remainder of this section will argue that CoHBAC is more accessible and knowable by design than the leading alternatives. CoHBAC is a unique combination of Role-Based AC (RBAC) and Attribute-Based AC (ABAC) which retains the flexibility to
implement either model exclusively or a hybrid based on user need and limitations. While RBAC (the dominant AC model applied in many provider-facing electronic health record systems) is commonly not considered to provide sufficient granularity for patient-controlled health information[10]; most patient centered AC models identified in the review provided some combination of role-based and identity-based policy statements. In the health care context there almost always exists a clear divide in roles between laypeople and professional providers which maps well into role based policy. However, an individual’s relationship with the various members of their CoH exist on a continuum of trust and therefore must be addressed on a case by case basis; this further emphasizes the users’ need to define AC policy with a high degree of granularity. Despite many users’ mental model of their privacy being more detailed than RBAC affords, some users cannot or will not bear the additional cognitive load. It is accepted that RBAC fails to provide a sufficient AC model for personal health but to design an alternative we must consider the potential users of a tool which would implement CoHBAC. We define our target user base as “Any individual actively engaged in managing their health.” This includes users whose needs range from those interested in casual personal health data management such as tracking fitness metrics to those actively undergoing treatment for their health concerns, both acute and long term. With a broad user base comes a wide variety of technical, physical, and mental skill sets. For this reason it is important for the proposed CoHBAC solution to be flexible and extensible by design such that a simplified model is accessible to users deficient in the required skills as well as an extended model for power users who may wish to define very specific policy, though not necessarily in the same application or interface. A broad user base also introduces a large variety of secondary actors with which the patient may have increasingly complex relationships. Dividing non-patient actors into trusted lay people and care providers simplifies the model by allowing for inherently more professionally trusted roles for primary care providers. However, the CoH extends past primary providers. It encompasses other dimensions of health care including policy makers and health authorities. An individual has constantly evolving relationships with these actors and thus an AC model that addresses the patients’ concerns must provide fine grained AC to express the current level of trust between the patient and each member of the CoH. To address the complexity of trust relationships, ABAC can be implemented to describe data and actors in a system. ABAC offers the ability to modify access policy at a fine granularity with the drawback of adding complexity for the user in both the initial setup and maintenance.
The complexity of ABAC stems, in part, from the difficulty for users to manage a mental model of the whole system over time. CoHBAC allows for patients to use user defined contextual groupings which relate directly to their perception of their CoH and health concerns. By closely coupling changes in the patient’s real world CoH or health concerns to correspond to required changes in their privacy controls CoHBAC can retain the fine grain control of ABAC while lessening the cognitive load on the user. The expectation is that patients can easily understand when they need to update their own access policy on a given circle as it will reflect changes in the state of their care context. In the CoHBAC model, individual actors are not granted access to data. Instead, actors can be members of one or more of a patient’s circles. This encourages patients to define contextual CoHs. The context of each circle may be defined by involvement in care for an illness or injury, or it may relate to a dimension of personal health such as fitness, diet, or mental health. A significant advantage of CoHBAC is that any instance of the model exists as a point on a continuum from lowest granularity (RBAC) to highest granularity (ABAC) inclusively dependant on the definitions of the circles. It is possible to implement RBAC and ABAC using CoHBAC. Generally, as the number of circles increases and the average number of members per circle decreases the model tends towards ABAC, where an instance with one member per circle and each actor only included in a single circle most closely resembles traditional ABAC. However, as the number of circles decreases and the number of members per circle increases the membership criteria becomes more abstract and the instance more closely resembles traditional RBAC.

In this section we have established how we have answered our first research question: “What is known in the current literature about AC models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility.” through a scoping literature review. We selected literature from reputable sources and utilized repeatable queries and controlled indexing terms. We presented ten requirements for developing patient centered AC models and Circle of Health based Access Control which meets those requirements.
4.2 Scoping Review on Requirements for Patient Privacy

4.2.1 Stage 1. Identifying the research question

In the pursuit of answering RQ1 we have developed a basis of knowledge about the domain and AC models therein. However, AC models alone are not sufficient to provide any guarantee of privacy to patients or allow them to be sufficiently informed to be aware of limitations. Health care is a complex and life-critical field in which electronic tools can make a significant impact\[2\]. Clinical care providers are dominantly concerned with the well being of patients but they are far from the only actor in this system. Developers of eHealth tools are also significantly responsible for how the interfaces and work flows guide users to make decisions. Not all actors may act in the patient’s best interest, PHI is valuable in many ways. In that way, even if an CoHBAC were implemented there is no guarantee the interface would faithful allow interaction with PHI if there were sufficient value in doing otherwise. This leads us to the second research question, RQ2,: “What are the requirements for access control and privacy controls in patient facing health systems with regards to creating comprehensible and maintainable privacy systems.”

4.2.2 Stage 2. Identifying relevant sources

We used the previously identified 3 sources for this review. Compendex and Inspec (accessed through engineering village) are used to find engineering literature. Pubmed was be used to search for medical literature. Only English language publications are reviewed. To better answer our research question with regards to the fast pace of technology we restricted our search to publications from the end of the first scoping review to date, from 2015-2018 inclusively.

4.2.3 Stage 3. Study selection

The diagram in figure 4.9 shows the results from the successive filtering steps applied. The queries applied were very similar to the previous review and are available in Appendix A. To further focus results, the controlled terms artificial intelligence, mobile telecommunication systems, computational theory, and embedded systems were also
Figure 4.9: The Scoping Review Process for Scoping Review on Requirements for Patient Privacy

The full queries for both Compendex and Inspec, through engineering village an pubmed are available in Appendix A.

The meta-data of each of the 340 query results was reviewed according to the following inclusion/exclusion criteria:

- [E1] - Exclude if meta-data (title/abstract/keywords) does not express any focus on consumer-facing health informatics applications. This may be expressed by mentioning a consumer-facing technology (such as PHR), a representative of such a technology (such as Google Health), the reference to consumers/patients as direct users of a system, or the use of terms that indicate a patient-facing component of the IT solution (e.g., Telehealth).

- [E2] - Exclude if meta-data does not express any focus on patient driven AC or
security models.

- [I1] Include otherwise

n=49 records remained after meta-data analysis. These records were subjected to a full text review by the following criteria:

- [I2] - Include if paper describes an AC model to the level of detail that allows the reader to formulate concrete AC policies, based on what is described in the paper.

- [I3] - Include if paper describes a formal model for reasoning / evaluating AC policies based on some notion of quality.

- [I4] - Include if paper describes user or other non-cryptographic domain requirements as a framework for future implementation of concrete AC policies.

- [E3] - Exclude otherwise

The resultant 22 publications are considered the corpus of this review. We subjected the corpus to full text analysis.

4.2.4 Stage 4. Charting the data

Following from our grounded theory approach each of the included publications were carefully reviewed and any mention of possible requirements were noted. Similar to the first review, we organized the tags into concepts and charted them using the CMap tool presented in figure 4.11.

As in the first literature review, all concepts are represented in the final list of requirements. However, not all concepts in figure 4.11 lead to additive properties to the identified requirements. For example, figure 4.10 is a subsection of figure 4.11 which features the concept of storage and shows that there are many types of data storage usable by eHealth systems. This influenced requirement thirty-nine: PHI requires reasonable cryptography, as each type of storage effects the advantages and risks of different cryptographic schemes. With future work it would be possible to identify more specific requirements which match to the chosen storage medium but as that is out of scope of this work we cannot make any recommendation as to what those relationships might be.
Requirement forty-one: Publishing of PHI must be privacy preserving, can be directly related to the privacy concept near the center of the concept map, shown in figure 4.12. User authentication, cryptographic protocol, data anonymization, and privacy policy are all identified as mechanisms which can contribute to preserving privacy. These techniques can be combined in various ways and may also incorporate mechanisms not identified in the corpus as long as the goal of privacy preserving data publication is met.

Spagnuelo & Lenzini’s literature review which mapped the properties and terms related to transparency in user centered systems was included in the concept map and is highlighted in figure 4.10[52]. Requirements forty-three through forty-nine can be sourced from these concepts as they concern verifiability and information accountability. Spagnuelo & Lenzini argue that data owners can be made aware of how PHI is stored, managed, and accessed by disclosing how the system works, i.e. increasing transparency. These themes were further reinforced by the work of Rezaeibagha et al. which highlighted the need for auditability and was extended in our work by relating it to Grumwell et al. and their work on policy-aware transaction logs[53].
4.2.5 Stage 5. Collating, summarizing and reporting the results

In this section we discuss the concepts that contributed to figure 4.11 and how they relate the literature in the corpus. We proceed to revise the 10 identified requirements from the first review based on the new domain knowledge. We conclude by presenting a more comprehensive list of requirements and Privacy Centered AC, our latest refinement on CoHBAC.

Healthcare Domain

AlThafi et al. comment that healthcare processes are complex, parallel, and have a high degree of variation as they introduce their approach to modelling healthcare processes using Business Process Management techniques[54]. A single care provider may fill multiple roles simultaneously in different contexts and have varied access to PHI within those roles[55]. Because of the dynamic nature of healthcare, unlike many other safety critical domains, it is difficult to limit access to resources based on work flow or context as rigidly defined procedures
may not reflect practice[56].

Alsalamah notes that healthcare if shifting from disease centered to a patient centered approach. This often results in a single patient interacting with many care providers. Patient centered care tools need to meet the needs of the care providers as well as the subjects of care[56].

Electronic health care, or “eHealth”, encompasses the use of electronic tools to improve health care. As Alsalamah states, eHealth is an umbrella term for all health systems with the shared goal of … facilitating shared informed decisions based on reliable information to improve the quality of care, patient safety, and outcomes. However, that information is highly confidential and sensitive and must be protected at all times [56].

Care provider and patients share information by sharing or centralizing an Electronic Health Record (EHR). According to Schiza et al. “The ideal EHR is defined as a collection of continuously updated health-related facts and medical data associated with a patient.”[57] and is visualized in figure 4.13. Sicuranza et al. adopt Kilic and Dogacs[58] definition of an EHR: An Electronic Health Record System (EHR-S) is a health information system whose aim is to collect and distribute electronic clinical documents and data about an individual’s lifetime health status.[59] Regardless of the precise definition of an EHR it is clear that the users of such a system may be spread across large geographic areas but still require timely delivery of PHI[60]. Providing accurate and quality features for EHR system services leads to better security and privacy protection for PHI[61].

Identifying relevant PHI can be a challenge, especially as the introduction of mHealth allows patients to create and interact with their PHI using mobile devices[62]. Prioritizing data from different sources with different credentials can be challenging and mHealth must balance its inherent ease-of-access with confidentiality[56]. As Grunwell et al. point out free-text is commonly used in clinical data entry but can be very difficult to analyze or process[53].

**AC Flexibility (Fine-Grain-ness)**

It is commonly agreed[62][60][59] that when patients are enabled to make AC decisions that they require fine-grain AC. According to [54] “The lack of FGAC is an open problem in HISs.” [63] suggests “The cornerstone of any successful
model needs to be flexibility and input from the patient”. FluxMED, studied in [53], is notable for its flexible approach to privacy management. Specifically, FluxMED relates tasks to workflows. “A flexible access control that meets each need of each individual is required in the healthcare domain” [54]. However, the trade-off of flexibility is complexity [55], which must be considered in this case so that patients can reasonably manage policy.

**Trusted Authority**

One strongly recurrent theme in the review was the basis that any HIT solution could and would be backed by a fully trusted central authority (CA) [55][53][64][65] despite the fact that few such central systems are reported on. These solutions may require legislative change and can potentially be costly to implement and maintain. Fernando et al. point out that, with the notable exception of Denmark, most European countries had abandoned their efforts to create a centralized PHI system, in part due to privacy concerns [4]. This includes the UK and France which already have significant investment into centralized public health services. Despite the lack of a legislative framework many authors suggest the possibility of a government CA [53].

[55] proposes the creation of a Global Medical Cloud (GMC) which would be a trusted policy and data storage intermediary. [64] and [65] offer privacy schemes reliant on a trusted CA, however, neither discuss how such a system
be implemented only that is must be trustworthy.

Storage systems need to provide access accounting services[52]. This poses a challenge in distributed systems such as storage cloud services. Significant work exists such as [66] which relies on a trusted Health Information Exchange (HIE) which enforces AC policy through management of the encryption scheme and provides accounting services. Similarly, [67] proposes using blockchain technology to create accountable ledgers for distributed storage. Access to the blockchain would be regulated by trusted Health care Data Gateways that act in the same way as trusted CA.

Health care is expensive, and when possible costs should be minimized[66]. This can be a motivation to reduce costs on PHI storage by using semi-trusted or untrusted services[65]. To combat the risk of a semi-trusted storage authority [64] base their scheme off storing and retrieving encrypted data to minimize or outright prevent storage systems from accessing plain text. [4] suggest going one step further and preventing semi-trusted storage authorities from linking access requests, PHI, and user or role.

Consent

Consent is an important aspect of medical care. It needs to be captured and saved based on contextual information. Because PHI is confidential, the only basis for accessing it is through that individual’s consent[62]. To maintain confidentiality, even when consent is given, the principle of least privilege should be applied[59]. Asghar & Russello go on to describe three kinds of consent in health care. Implicit consent, given through ones actions; explicit consent given by a patient or guardian; and informed consent which requires the patient to understand the procedure they are about to undergo[62].

While not all patients can manage their privacy there are patients that can and desire the ability to[53]. Patients also have the right to make decisions regarding the collection, use, and disclosure of PHI[62]. While some patients may have difficulties with the cognitive burden of managing their privacy concerns, the ability to define views on PHI simplifies management for the owner or curator[59].

Patients have the right to withdraw or revoke consent[64]. This is a difficult and costly problem with paper records which many new privacy schemes attempt
to solve[62]. One major way electronic systems reduce costs is by reducing the need for paper consent. E-consent can be issued by a patient as an authorization policy[62]. Despite the additional cost savings of automating consent it cannot be fully automated and requires some form of human review[63][62]. Patients require an understandable, affordable, and accessible mechanism to give explicit consent, potentially requiring multiple authorized request makers[61]. Controlling consent can be improved by bring the necessary tools closer to the data subject[62]. Data security, especially with shared PHI or provider tools accessed in public spaces, is essential to maintain the access rights the patient has consented to[66].

There are times when consent policies conflict and, due to the complexity of consent, they cannot be automatically resolved. Individuals consent may conflict with societal needs such as the desire to aggregate large amounts of PHI to identify population scale health trends[62]. An individual’s consent may also conflict with the health outcomes of others such as in the case of those with infectious diseases[63]. Ultimately, it is clear that capturing and maintaining up to date patient consent is a nearly impossible physical task and, to date, still a difficult electronic one.

Emergency Consent (Break-the-glass)

In health care systems the delivery of care comes first and nothing should interfere with it[55]. Or as Shrestha et al. put it “The goal of health care systems is to deliver the greatest health service for anyone from anywhere”[66]. This includes patient privacy. Patients who are unable to respond in emergency situations may have PHI which, if disclosed, can improve patient outcomes in the hands of first responders and care providers. Health care access should operate under the “need-to-know” principal, but in practice a care provider may not know what PHI is being withheld[54].

According to Bhuyan et al. “...a need exists to find a balance between the rights and desires of the patient and the need for complete patient information to provide high-quality patient care and to safeguard the health of the general public.”[63]

Gope et al. state that traditional AC is based on the principle that access requests are known in advance. This can make them slow to react to dynamic
situations. “However, since in health care systems an essential requirement is that delivery of care comes first and nothing should interfere with it.” Huynh et al. also agree that AC must ensure the patients privacy, not hinder care providers or endanger the patients life[68].

Gope et al. state minimum security requirement should never be circumvented, even in an emergency and that break-the-glass policies should always require a user obligation in some form to justify use and make them responsible[55].

[69] and [62] both incorporate emergency access into their models. Both also propose activating an emergency mode or module by shaking a personal mobile device.

**Information Accountability**

Information Accountability (IA) protocols can be used ...to enforce appropriate use through after-the-fact accountability for intentional misuse[53]. Grunwell et al. propose a scheme which meets the need for open access for care providers and mitigates the risk through IA. It is important for the system to clearly communicate that actions are being recorded and will be reviewed to discourage curious insiders. Users need to be held accountable for their actions[53]. Each operation to PHI should be verifiable, accountable, and immutable[67]. To accomplish this PHI storing systems must be auditable[61] and keep policy-aware transaction logs[53].

Patients should be empowered to own, control, and audit their PHI and related access[52]. Not only should PHI access logs be available for data owners and custodians to audit[4][64], but should be provided in a user friendly format[53].

Al-Aqeeli et al. propose a scheme based on risky access[70]. Risky access can be granted, within some defined acceptable level of risk, when risk mitigation techniques are applied to reduce said risk. After risky access PHI should be acknowledged as being only as private as that access allows.

**Data Requester Goals**

Many individuals and groups want access to PHI. Some individuals make requests based on their personal relationship, or role, to the patient[55]. Legitimate access requests can be accompanied by purpose for the request including:
their goal or context, or length of time access will be required. Regardless of reason or context most parties who access PHI want to maximize their data access. This can be a motivation behind legitimate data request makers wanting systems with unrestricted access to PHI even if user obligation is required.

There are many legitimate reasons to want access to large amounts of PHI, such as: predictive data mining techniques, the research and implementation of effective Clinical Decision Support (CDS) tools, and broader access for research leads to a better understanding of public health.

Zhang et al. propose an AC scheme based on care providers being alerted to access and directly negotiating access with the patient to help legitimate caregivers maximize access.

While caregivers want to maximize their access they generally want to do so without being exposed to litigation or compromising their work flow i.e., preferring free-text to structured fields which lend themselves better to data science techniques.

Data Owner Privacy Goals

There is an increasing demand for patient control over PHI worldwide. Liu et al. claim that patients who have full access to their PHI can better grasp their health status. In order for patients to feel in control of technology they must be educated on how the technology works and being able to audit those systems; this is the responsibility of the technology.

Data owners need to be engaged with their privacy tools for a patient centered system to be effective. Data owners can better protect their privacy if they are able to enforce new access policy in real time. This drives a demand for patient centered AC from those who are informed about it and capable of leveraging such a service.

Controlling PHI can be more important, although, more difficult, for patients managing multiple health concerns. Some patients may be co-morbid, meaning they are managing more than one health concern, possibly with more than one care team. Co-morbidity is also more common in older patients who typically have less experience, skill, and capacity with newer technologies.

Once a data owner is in control of their PHI they are exposed to more
risk. Social engineering attacks, user error, or honest-but-curious legitimate insiders can more easily gain access to private information. More recently, the risk of disclosing data for the sake of aggregation is difficult to explain to data owners. Users typically cannot understand the risks of disclosed data being aggregated[62]. Additionally, in the case of access being revoked or withheld, the very act of instating new policy could potentially endanger the individual. As such, it is important that data request makers not be aware when access is withheld or to what extent it is withheld[63].

Availability

Health systems must be highly available[59][67]. According to Bhuyan et al. pertinent integrated access is one of the goals of eHealth[63]. Clinical data must be available to avoid inaccurate decision making[53]. Alsalamah illustrates a scenario involving a latex allergy in which easily avoidable mistakes were made resulting in declining patient health outcomes[56]. Some systems are safety critical and typically expect instantaneous availability of accurate PHI in order to make good clinical decisions[69][61]. PHI must be backed up and recoverable[67][61].

Scalability

PHI storage mediums needs to be scalable[61]. As Schiza et al. state “The EHR can be a dynamic electronic record that chronologically stores a citizen’s medical data from approximately nine months before birth to their death”[57]. This definition refers to traditional EHR systems but modern mobile sensors also create specialized health networks that allow an individual to generate large amounts of PHI not directly related to their involvement with registered medical associations. In either case, PHI naturally grows larger over if a patient interacts with the system.

It is important that the performance of a PHI storing system also be scalable[4]. Consent schemes must be computationally feasible[64]. In mHealth reducing the load on sensors can be valuable to longevity.

Scalability while maintaining privacy and accountability is an open problem in HIT. Many technologies are currently being used to improve scalability in privacy privacy such as: blockchain [67] for accountability through sue of the
public ledger and transaction validation, scalable encryption techniques[66] and key sharing schemes[60], and how FGAC can be used to improve scalability in cloud environments[61].

**Transparency**

Spagnuelo & Lenzini conducted a literature review to map the properties and terms related to transparency in user centered systems[52]. They identified relationships between various concepts related to transparency, this is presented in figure 4.14. They performed this survey based on the notion that “Transparency is also a quality that is believed to realize peoples right to privacy”[72]. Data owners should be aware of how PHI is stored, managed, and accessed. Systems can achieve this by disclosing how the system works in terms of informational sources and access requests. Transparency intends to simplify the understanding of complex privacy policy. Transparency and accountability are “critical to helping society manage the privacy risks that accumulate from expeditious progress in communication, storage, and search technology”[73]. Privacy, when applied to transparency, is a principal of minimal exposure. Users of a system should be aware how to minimize disclosure to accomplish their goals[52].

![Figure 4.14: Spagnuelo & Lenzini Properties related to Transparency](image-url)
Interoperability

Health Information Exchanges (HIE) are often implemented in HIT[66]. HIEs attempt to reduce medical errors through increased interoperability. As among the causes of medical errors are conflicting treatments and incomplete information[4]. In general, patient centered care requires more open information sharing than traditional care teams[56].

As established, with increased disclosure comes significant risk of privacy breaches to the patient which should be mitigate with IA and/or user obligation. However, third parties may still manage storage of PHI which exposes them to additional information such as metadata[61], access request and identity/location linking[4], or management of cryptographic protocol allowing access to plaintext[64].

PHI should not be trusted to third parties[67]. And health systems must avoid integrating with untrusted or non-legitimate systems[61]. Despite the risks of open sharing of PHI patients are able to securely control their data from their mobile device[62], which may be necessary to cope with an aging population in many parts of the world[56].

Threat Modelling

There is a significant body of work on threats to storage of sensitive information. Managing firewalls and other critical network resources helps prevent unauthorized access[66]. PHI is not only vulnerable from outside attackers but also suffers from many distinct disadvantages which attackers can take advantage of[71].

PHI must be secured against those storing it[66]. Ideally PHR providers should not be trusted and should provide end-to-end source verification[65].

The less restrictive access require for patient centered care also creates more opportunities for insider attacks. Internal attackers can be classified as: accidental, honest-but curious insider, and data breach by an insider[53]. PHI can often be leaked unintentionally, or due to negligence on the part of a data custodian[64]. Patient centered tools, such as AC, cannot easily defend against users who misuse legitimate access[70]. This can include the need for care providers to access PHI in public areas, such as hospital work stations, or disclosure to proximal patients or care providers lacking consent[56].
Data Breach Contingency

Simply keeping access logs is not enough to secure PHI. Both Rezaeibagha et al. [61] and Shrestha et al. [66] agree that PHI access must be monitored for suspicious activity helps eHealth systems achieve positive patient impacts. Grunwell et al. and recommend deterring honest-but-curious insiders by use of disincentives, such as penalties [53]. Regular review and deterrents can reduce misuse by legitimately authorized users [74]. Regardless if breached by an external attack or an insider data storage owners should be required to give timely notification of data breaches [52]. Timely notification of illegitimate disclosure may be required to prevent further damage to the victims [74]. Failing to act responsibly may result in storage systems being litigated for damages or fined by the state when a data breach occurs in part due to their negligence [63].

Cryptography

PHI requires a reasonably secure cryptography [57]. PHI privacy is typically preserved by privacy policies, cryptography, or a combination of the two. Sufficient cryptography improves privacy [70].

There are two high-level goals to encrypt PHI. To establish a secure communication channel and recipient identity before exchanging PHI [61]. And to ensure that only legitimate data requesters can view accessed PHI [66]. Data owners rely on AC systems to allow them to define legitimate use. In storage, AC mechanisms are dependent on encryption techniques for enforcement [65][60][61].

Anonymization

PHI can be anonymized by storing it in such a way that the identity of the owner of the data is not exposed even if the remaining data is. Data anonymization techniques can be applied before PHI is exposed to improve privacy [70]. Schiza et al. assert that publishing of PHI needs to be privacy preserving. PHI can be anonymized in such a way that the storage owner cannot related stored records and identities [67][69].

In addition to data anonymization, access records may reveal important details about either the identity of the request maker or the nature of the stored PHI [4]. Data aggregation may undermine data anonymity with knowledge of the access history [62].
Trust in HIT

There are at least two types of trust in health care when dealing with HIT systems. The degree of trust between patients and their care providers. Providers rely on patients to be open and truthful to provide the highest quality of care. Patients without sufficient trust in their care provider may choose not to disclose PHI. There is a second kind of trust is between patients and the HIT systems, trusting it not to be breached by malicious attackers[63]. Patients with low trust in HIT systems may be reluctant to share PHI then for any other purpose than direct clinical care[61]. Patients with incomplete PHI can more easily be the victim of medical errors[4].

Authentication

Good authentication is a prerequisite for reasonable security. Systems controlling PHI require reasonable authentication[57]. Due to the sensitivity of PHI, HIT systems are a good candidate to use multi-factor authentication (MFA) schemes to improve authentication[69]. Furthermore, personal digital signatures could be used to improve authentication as well as data providence and integrity if successfully implemented[57].

Data Integrity

Integrity of data is a cornerstone of the security triad. Authenticity and integrity must be maintained for PHI, especially if it is shared[61]. Data recipients should be able to verify PHI integrity through some secure mechanism[64]. Contextual or dynamic data, such as that from mobile sensor networks, must also be captured correctly for patients and care providers to react appropriately[62].

Legislation

Legislation about PHI seeks to establish a common set of principles for protecting privacy for data under its jurisdiction[62]. Robust policies and regulations can facilitate secure sharing of PHI[61]. Many countries have established a legislative framework for data protection, PHI requires a legislative framework to be reasonable secure[57]. These legislative frameworks may require data owners to share data with the government or third parties, possibly against the owners
wishes[64].

Live Communication

With the level of connectivity available to many patients, it is possible to for them instantaneously receive and generate alerts. While this has traditionally taken the form of call bells and emergency services to receive direct care, it is possible to engage patients when their PHI is accessed[64]. Potentially more importantly, HIT systems can alert data owners of invalid access requests. This can open communications channels to allow patients to engage request makers to determine legitimacy and have them justify their access request[53]. Within the larger care team, individual care providers can also use these types of alerts as well as generating their own to update colleagues or the patient to new information in a timely manner[56].

4.2.6 Refinement of First Scoping Review Requirements

[R1] Differentiate data by sensitivity

It was commonly agreed that PHI has different levels of sensitivity[70][55][69][54][71]. Sensitivity levels may be related to level of urgency[56]. Patients may even find that having multiple control levels allows for easier management of AC policy[59]. Sensitivity levels may be implemented broadly, differentiating clinical from non-clinical data. PHI could also be differentiated by care context, that is, some data types such as PHI referring to sexual health history, may be considered to be more sensitive than others, such as general demographics data. To fully meet the needs of all potential users the users themselves should be able to define sensitivity levels.

[R2] Differentiate data by type or treatment (episodic) context

PHI can be generated about a specific encounter with a care provider, a treatment or procedure, or managing a health concern ongoing. PHI needs to be differentiable by these types, which change as a patient progresses through the stages of a treatment[54]. Patients who are aware of the relationships between their PHI and health care interactions can be informed of the purpose of PHI access[62]. A set of predefined attributes may not be sufficient to capture a
patients privacy concerns or describe the contextual information relevant to the clinical decisions[62]. Patients may want to describe privacy policy based on contextual factors which must be measured at the time of access[75]. Therefore, PHI, and related access policy, should allow policy based on dynamically generated information associated with the access request[59]. Asghar et al. describe such a system using policy templates, privacy policy which is instantiated by variables based on contextual data. Policy templates allow for dynamic sensor measurements, such as GPS, and role assignment, such as a doctor filling the role of emergency responder[62].

[R3] Maintain data provenance (origin, time of creation, time of last access)

Often with traditional clinical PHI, data owners are not the data creators[52]. PHI creators may have different medical credentials, or lack thereof, therefore it is important to maintain data providence.

[R4] Provide data compositionality

Data compositionality is consistent with the episodic and context related treatment workflows in healthcare. Data compositionality is mandatory for patients to be able to grant partial access to PHI[64].

[R5] Subjects may be individuals or entire organizations

Requestors may be individuals clinics, or larger organizations. In some jurisdictions, such as the US, groups such as healthcare providers and insurance companies must be able to request a patients PHI[64]. Researchers and research groups may also require access to PHI[75].

[R6] Subjects may be allowed to view or contribute data to a patients PHI

As consent for a patient is required before a patient is able to give it, and may continue until after a patient can no longer, patients may delegate privacy control and treatment decisions to a custodian or have a guardian appointed[63]. There may be more than one owner for a piece of PHI[57].
[R7] Differentiate CoC by trust criteria. (Patients may have multiple CoCs)

Patient health and trust relationships are dynamic[4]. Patient may desire privacy policy informed by calculated trust metrics, denying access to even authorized users when they are trusted enough by the patient or HIT system[71]. A trust metric can be based off past direct and indirect interactions with a user and can incorporate user feedback[71][70]. Dynamic trust systems are often referred to as reputation management systems and are employed to establish a level of trust in relationship-based AC models[74]. AC models incorporating trust metrics are more adaptable and dynamic in responding to access requests[70].

[R8] Allow for ephemeral CoCs as well as for persistent ones

Healthcare is episodic. The PHI generated by and for healthcare can be needed based on emergency or stage of treatment. Consent should be able to be similarly temporally bound[62]. In some legislative frameworks PHI may need to be destroyed after a time frame, end of intended use, or change in owner status[62].

[R9] Subjects are allowed to stay anonymous with respect to other subjects in the CoC Usability

Very little additional information was uncovered related to this requirement. This may be because the focus of this work was on the patient who is the subject of care and less so on the privacy needs to the other actors in their system. Fernando et al. specifically outline that access records not be linkable to PHI owners[4]. Asghar et al. caution that data aggregation of access records may undermine anonymity techniques and reveal sensitive details about the nature of stored PHI[62].

[R10] The AC Model should be easy to use and comprehend from a patients perspective

This requirement is inherently difficult to define and meet in the scope of the original work, which was specifically on access control. Some of the corpus indicated that users ability to understand and use the tools provided was linked to the success of AC scheme implementations. Bhuyan et al. discuss the challenges
of how costly and time consuming it is to inform patients to consent to medical procedures[63]. They go on to suggest that IT systems may have a better chance of communicating a clear understanding of how AC and their interactions with HIT can affect their care.

This work seeks to view patient privacy as a larger technical system in need of clear definition. As such it is important to recognize that while AC is the underlying mechanism for managing privacy policy, reasonable user centered privacy cannot be met by AC alone. Privacy self-management tools must be accessible and understandable. Privacy policy should be presented to users in a way that is easy for to understand[62]. The user facing interface, and its associated functions and services, as well as education/practical learning/intuitiveness play an important role in determining if a user can comprehend and express their desired privacy policy in an actionable and timely way.

PHI consent policies must constantly weigh ease-of-access against privacy[62]. Data owners need to be understand the risk and repercussions of a PHI data breach to be informed decision makers[63]. In addition to risks, data owners also need to understand the preventive measures in place to protect their PHI privacy[52]. This is a key patient motivation for transparent medical systems. That privacy self-management tools and notices need to lead patients to make rational, informed decisions[62]. Data owners should understand what will happen to their PHI as well as what has happened to their PHI[52].

Designing systems which have a high degree of usability is challenging. To provider comprehensible and easy to use systems often requires many iterations and rounds of user testing. Systems such as those proposed by: [55],[53],[64],[65] which design around a central authority to serve longitudinal health records throughout the life of the patient would be particularly difficult to design for due to the diverse society of actors in health care systems with differing, and specific, privacy needs[4].

Users must use an interface to interact with their AC, as well as any other user facing privacy tools. AC interfaces should be simple and intuitive[59]. This can conflict with the need for expressiveness in the system when some users are willing and capable to proactively manage privacy and some are not but still gain to benefit from using the HIT system. Some users may require a simplified AC management interface [59]. It can be inferred that a single HIT tools may benefit from having multiple specialized interfaces for data owner and custodian
interaction with privacy tools. Using a goal driven approach, which CoHBAC is with contextual circles, can simplify privacy policy for users[62]. Asghar et al. go on to say that user goals and context considerations make access policy more maintainable.

4.2.7 Synthesized Requirements

After identifying concepts and categories we present the following list of requirements as the result of the scoping literature review.

<table>
<thead>
<tr>
<th>ID Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Connection requests must be reasonably authenticated</td>
</tr>
<tr>
<td>2</td>
<td>Should disclose authentication process</td>
</tr>
<tr>
<td>3</td>
<td>Must establish a secure communication channel with any actor</td>
</tr>
<tr>
<td><strong>Data Verification</strong></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Must have a mechanism to verify the integrity of stored and retrieved data</td>
</tr>
<tr>
<td>5</td>
<td>Must avoid integrating with untrusted systems</td>
</tr>
<tr>
<td><strong>Storage Availability</strong></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Must grant access to PHI in a timely manner</td>
</tr>
<tr>
<td>7</td>
<td>PHI storage must be scalable</td>
</tr>
<tr>
<td><strong>Data integrity</strong></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Storage should not alter stored PHI</td>
</tr>
<tr>
<td>9</td>
<td>Storage should not have access to unencrypted PHI</td>
</tr>
<tr>
<td>10</td>
<td>PHI must be backed up and recoverable</td>
</tr>
<tr>
<td>11</td>
<td>Reasonable network(external) security is required for storage of PHI</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continued on next page</td>
</tr>
<tr>
<td>ID Number</td>
<td>Requirement</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>12</td>
<td>The access control scheme must be sufficiently expressive to allow data owners to express privacy policy without compromise</td>
</tr>
<tr>
<td>13</td>
<td>Access Control should allow differentiation of PHI by sensitivity</td>
</tr>
<tr>
<td>14</td>
<td>Access control should allow differentiation of PHI by user defined contextual groupings</td>
</tr>
<tr>
<td>15</td>
<td>Access control should allow policy based on dynamically sensed criteria</td>
</tr>
<tr>
<td>16</td>
<td>PHI must maintain data provenance</td>
</tr>
<tr>
<td>17</td>
<td>Access control must allow compositional PHI</td>
</tr>
<tr>
<td>18</td>
<td>Each operation to PHI should be verifiable</td>
</tr>
<tr>
<td>19</td>
<td>Each operation to PHI should be accountable</td>
</tr>
<tr>
<td>20</td>
<td>Each operation to PHI should be immutable</td>
</tr>
<tr>
<td>21</td>
<td>Individual actors may be professional care providers or trusted laypeople</td>
</tr>
<tr>
<td>22</td>
<td>An actors may represent an individual or entire organizations or groups</td>
</tr>
<tr>
<td>23</td>
<td>Access control should allow for persistent and ephemeral groups of actors</td>
</tr>
<tr>
<td>24</td>
<td>Data owners may have a designated guardian</td>
</tr>
<tr>
<td>25</td>
<td>Data custodians may be granted all, or some, of the abilities of a data owner</td>
</tr>
</tbody>
</table>

**Access Requests**

<table>
<thead>
<tr>
<th>ID Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>PHI may have more than one owner</td>
</tr>
<tr>
<td>27</td>
<td>Access requests by data owners must be granted</td>
</tr>
<tr>
<td>28</td>
<td>By default, only the data owner should have access to PHI</td>
</tr>
<tr>
<td>29</td>
<td>Data owners must be able to authorize others to access PHI</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>ID Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Purpose of use must be included with access requests</td>
</tr>
<tr>
<td>31</td>
<td>Unauthorized actors should not be aware when access is withheld or to what extent it is withheld</td>
</tr>
<tr>
<td><strong>Consent Precedence</strong></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Access control should provide a mechanism to overturn implicit consent to provide care to that individual (break-the-glass)</td>
</tr>
<tr>
<td>33</td>
<td>Access control may provide a mechanism to overturn explicit consent to provide care to that individual</td>
</tr>
<tr>
<td>34</td>
<td>Access control must not provide a mechanism to overturn informed consent to provide care to that individual</td>
</tr>
<tr>
<td>35</td>
<td>Access control may provide a mechanism to overturn consent which conflicts with another patient’s care</td>
</tr>
<tr>
<td><strong>Policy enforcement</strong></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Data owners must be able to find out how privacy policy is enforced</td>
</tr>
<tr>
<td>37</td>
<td>Access control must support access revocation</td>
</tr>
<tr>
<td>38</td>
<td>Consent schemes must be efficient as not to reduce availability</td>
</tr>
<tr>
<td><strong>PHI Publishing</strong></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>PHI requires reasonable cryptography</td>
</tr>
<tr>
<td>40</td>
<td>Identifying information must not be disclosed to untrusted systems</td>
</tr>
<tr>
<td>41</td>
<td>Publishing of PHI must be privacy preserving</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>ID Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>Stored PHI should be anonymized</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>PHI storing systems require reasonable risk mitigation</td>
</tr>
<tr>
<td>44</td>
<td>PHI storing systems must keep policy aware access request logs</td>
</tr>
<tr>
<td>45</td>
<td>PHI storing systems must clearly communicate that actions are being recorded</td>
</tr>
<tr>
<td>46</td>
<td>PHI storing systems must have a deterrent, such as penalties, for improper use</td>
</tr>
<tr>
<td>47</td>
<td>PHI storing systems should be publicly auditable</td>
</tr>
<tr>
<td>48</td>
<td>Access logs must be monitored to identify suspicious activity</td>
</tr>
<tr>
<td>49</td>
<td>Data owners need be given timely notification of data breaches</td>
</tr>
<tr>
<td><strong>Terms of Use</strong></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Data owners must be informed when their data is collected, used, disclosed, or aggregated</td>
</tr>
<tr>
<td>51</td>
<td>Data owners must be informed of how their PHI is stored, managed, and accessed</td>
</tr>
<tr>
<td><strong>Privacy Control Interface</strong></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Data owners must have access to an interface to manage privacy policy</td>
</tr>
<tr>
<td>53</td>
<td>Data owners need to be able to enforce new privacy policy in real-time</td>
</tr>
<tr>
<td>54</td>
<td>Privacy control interfaces must be intuitive</td>
</tr>
<tr>
<td>55</td>
<td>Data owners may require a simplified interface</td>
</tr>
<tr>
<td><strong>Client Usability</strong></td>
<td>Continued on next page</td>
</tr>
</tbody>
</table>
Table 4.2 – continued from previous page

<table>
<thead>
<tr>
<th>ID Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>Data owners need to be engaged by their privacy tools</td>
</tr>
<tr>
<td>57</td>
<td>Access logs need to be presented to data owners in a user friendly manner</td>
</tr>
<tr>
<td>58</td>
<td>Privacy controls must be understandable to data owners</td>
</tr>
<tr>
<td>59</td>
<td>Consent systems must be accessible</td>
</tr>
<tr>
<td>60</td>
<td>Client should alert data owners to information relevant to managing PHI</td>
</tr>
<tr>
<td><strong>User education</strong></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Data owners must be educated on the risk of misused legitimate access</td>
</tr>
<tr>
<td>62</td>
<td>Data owners must be educated on the risk of a security breach and how to minimize damage should one occur</td>
</tr>
<tr>
<td>63</td>
<td>Data owners must be informed of PHI security and risk mitigation</td>
</tr>
<tr>
<td>64</td>
<td>PHI management tools need to lead data owners to make rational decisions</td>
</tr>
<tr>
<td><strong>Sensors</strong></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Sensors must be accurate and trustworthy</td>
</tr>
</tbody>
</table>

Table 4.2: Identified Requirements from Second Scoping Review

4.2.8 Privacy Centered Access Control

In this section we will present a refinement of the CoHBAC model in figure 4.15. We name this new model Privacy Centered AC(PCAC) to better represent its generalizability. PCAC simplifies and refines the foundational concepts of CoHBAC. CoHBAC was designed and argued to meet the requirements identified
in the first literature review. This review extends the scope beyond a single privacy mechanism, like AC, to a systems view which includes AC as a one of a series of interconnected components. During the review, evidence was gathered to further refine the requirements from the first review. The AC model is not capable of meeting all the requirements from the second review, however, there is a subset specifically intended for AC, [R12] through [R25]. PCAC is is able to meet the original requirements as well as the relevant requirements from the second review

PCAC is a hybrid approach that allows writing policy which includes both static and dynamic attributes. A hybrid approach is the most flexible. We require a high degree of usability in many applicable health care scenarios. The data requirements identified in developing CoHBAC and have also been met by PCAC. CoHBAC is compositional by design and PCAC preserves that.

Like its predecessor, PCAC is a graph based AC model. One way of specifying a secure AC model is to define a secure initial state and a set of secure transformations that are guaranteed to output a secure system state given that
their input is a secure system state. We will further discuss PCAC in terms of the relevant requirements in Chapter 6 when we develop a hypothetical model in which PCAC would be implemented.

We have now presented the requirements identified from codifying the second corpus and the refinements of the requirements from the first corpus. We propose that meeting some or all of these requirements will benefit eHealth systems from a patient privacy perspective. We also have presented PCAC as the successor to CoHBAC which is more fit to meet the new requirements. To better discuss the requirements and their implications, in chapter 5 we organize these requirements with a conceptual model of accountability we identified from the literature reviews. We name this four piece model the Patient Centered Privacy Framework.
Chapter 5

Patient Centered Privacy Framework

Accountability was a strongly recurrent theme in the review. The question of who is responsible for accidental disclosure, breaches, or other failures resulting in harm to patients. We have categorized the identified requirements into the Patient Centered Privacy (PCP) Framework to model privacy concerns of data owners. This framework decomposes patient centered eHealth systems into four components: a Trusted Service Provider, Health Information Exchange, Storage, and Clients. We model the relationship between these components in figure 5.1.

The PCP Framework is intended to be used to model eHealth systems and to better understand to what degree patient privacy is being protected. In the case of a breach, the PCP Framework can be used to model and understand where privacy policy/tools have failed and who is accountable. The PCP framework can be used to model a wide variety of eHealth systems. There are many use cases for instances of the PCP framework such as: examining eHealth in different jurisdictions, under different businesses models, or uncover underlying assumptions. The PCP framework can also be used in developing privacy preserving systems by software architects. The framework requirements function as a baseline for providing privacy and backing up that claim to potential users and interested parties.

The PCP Framework encapsulates the requirements identified from the reviews. We present the breakdown and core responsibilities in table 5.1. PCP
system requirements are reflected to some degree in many eHealth contexts and can be implemented utilizing an array of technologies. Here, we will discuss how each of these requirements can be met in a general sense. We note that how a given eHealth system meets one requirement may necessitate some further restriction in others. For example, distributed cloud storage has additional cryptographic concerns, and while it may be used to effectively meet storage requirements, additional knowledge and expertise are needed to choose a reasonably secure encryption scheme. Again, these trade offs will not be examined in detail in this work but considered a specialization of the model to be discussed in the future.
<table>
<thead>
<tr>
<th>Component Name</th>
<th>Core Responsibilities</th>
<th>Associated Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Service Provider</strong></td>
<td>-Accountable</td>
<td>[R1]-[R5]</td>
</tr>
<tr>
<td></td>
<td>-Service architecture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Determines trustworthiness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-First contact with data owners</td>
<td></td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>-Highly available</td>
<td>[R6]-[R11]</td>
</tr>
<tr>
<td></td>
<td>-Recoverable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Physically secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-High data integrity</td>
<td></td>
</tr>
<tr>
<td><strong>Health Information Exchange</strong></td>
<td>-Highly available</td>
<td>[R12]-[R49]</td>
</tr>
<tr>
<td></td>
<td>-Appropriate network security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Internally and externally accountable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Privacy preserving data publishing</td>
<td></td>
</tr>
<tr>
<td><strong>Clients</strong></td>
<td>-Lead data owners to make rational decisions</td>
<td>[R50]-[R65]</td>
</tr>
<tr>
<td></td>
<td>-Understandable and intuitive interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Allow interaction with data and privacy policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Educate and empower data owners</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.1: Components of PCP Framework
5.1 Trusted Service Provider

The Trusted Service Provider (TSP) is intended to represent the business, government, or independent group with which a data owner enters a contract, either implicitly through use or more formally through contracts, for that group to provide storage, access, and/or other services for PHI. The TSP defines relative trust in PCP systems. Data owners may engage directly with the tools provided by the TSP, such as fitness tracking services, or indirectly, such as care providers who use clinical tools to benefit the data owner.

The TSP is accountable to the data owner. And while they may make contracts with other service providers, such as a storage services, it is expected they will be pursued by data owners foremost for any damages. The TSP may choose to directly manage PHI technologies. The TSP may also contract other service providers, provided they are held accountable to the TSP just as the TSP is to the data owner. The TSP may also contract with semi-trusted services provided the risk is reasonably mitigated, this will be discussed in more detail later. The must facilitate and authenticate the communication between all parties by [R1] ([R1]Connection requests must be reasonable authenticated) and [R3]([R3]Must establish a secure communication channel with any actor) though they may empower another authenticated actor to do so after initialization. Disclosing the authentication process, without compromising security, by [R2]([R2]Should disclose authentication process) facilitates building trust between all actors in the system, not just between the actors and the TSP. Information disclosed by [R2] should not compromise security.

PCP in its simplest form can be visualized as a single physician clinic using paper based records. The clinic is a trusted service provider who manages their own paper storage and all access manually as to act as the Health Information Exchange. Whatever the medium, the trusted service provider has a direct trust relationship with data owners and breaking that trust may result in patients no longer storing or generating PHI on that system. Because providers must build and maintain trust relationships with data owners, it is not unreasonable to expect providers of such a service to meet [R5]([R5]Must avoid integrating with untrusted systems) as they should be aware of the sensitivity of PHI and take reasonable steps to protect it by requiring some standard of trustworthiness. Furthermore, the TSP should understand the clinical need for PHI data integrity
and meet [R4] (Must have a mechanism to verify the integrity of stored and retrieved data) if they maintain their own storage and even more so if they do not, which we will discuss shortly.

5.2 Storage

The storage system in this framework is typically regarded as dumb storage. That is, decision making, privacy policy, and cryptographic techniques are responsibilities of other parts of the system and the storage is just that, the physical (centralized or distributed) storage medium and the direct interface which is used to store and retrieve PHI. It is well established that the following requirements must be met to provide high quality, reasonably secure storage of PHI, or any sensitive information: [R6] (Must grant access to PHI in a timely manner), [R8] (Should serve unaltered stored PHI), [R10] (PHI must be backed up and recoverable), [R11] (Reasonable network (external) security is required for storage of PHI). Furthermore, it has been discussed that PHI is rarely a fixed size and typically will grow over the lifetime of the patient, so we add [R7] (PHI storage must be scalable) as specific to data of this kind.

In some cases the TSP may store PHI on semi-trusted or untrusted storage mediums. In these cases it is not reasonable to expect that storage provider to faithfully meet [R8], for this reason, as well as when there are unintentional storage and retrieval errors, it is the responsibility of the TSP to meet [R4]. It is possible to store sensitive PHI on semi-trusted storage, through data anonymization and other data privacy preserving techniques on the part of the HIE. Even with trusted storage there is always a chance of physical breach, successful network, or social engineering attack which allows attackers to gain access to large amounts of stored PHI. Thus in many scenarios there is a significant security advantage to meeting [R9] (Should not have access to unencrypted PHI). Necessitating encrypting and decrypting every storage and access request can become computationally expensive. While significant work exists investigating more efficient encryption schemes for data like PHI, there is also the potential option of physically inaccessible storage, secure data warehouses. A TSP or HIE could reasonably prevent on-site access to the storage medium to untrusted individuals or use some form of cold storage technique to reduce exposure to external attackers while still having access to plaintext PHI. This model, while
often seen in practice, requires rigorous security procedure to be followed at all times because of the nature of PHI, once PHI is published it can not be made private again, meaning it would only take one lapse in security protocol or an unexpected attack to violate [R9]. In an ideal system the information would be reliably anonymized despite the computational cost.

5.3 Health Information Exchange

The Health Information Exchange (HIE) is the, typically digital and remote, point of contact between actors in an eHealth system (through a client) and stored PHI. The HIE cannot be untrusted as it manages general security of PHI and, by definition has access, to plain text PHI. If a HIE is compromised a significant amount, if not all, of the stored PHI would be disclosed due to the breach in the cryptography scheme. The TSP may directly manage the HIE or it may be a separate entity, even an establishment, and empowered by the TSP. The TSP and HIE may subscribe to some mutual system of trust or one of the TSPs choosing.

5.3.1 HIE Cryptography

The HIE allows actors in a system, through a client or clients, to interact with their own PHI and potentially request information from others. It is a given that increased sharing among care providers increases health outcomes, especially in the context of a single patient. Managing PHI and maintaining privacy requires both network security between the client and HIE and storage security, although this may be the same scheme. This is true of any sensitive data, even stored passwords, and it is a given that the HIE would provide [R39]([R39]PHI requires sufficient cryptography). Furthermore, sufficient cryptography must include the ability to revoke access, by [R37]([R37]Patients need to be able to revoke access), which a poorly designed scheme for PHI cannot do. Despite the complexity of cryptographic schemes for PHI they must also maintain a high level of scalability by [R38]([R38]Consent schemes must be efficient enough to not impact availability). This is a common tradeoff made to reduce costs, as is a lack of anonymization in stored PHI, however, there is a clear benefit to doing so to protect privacy so the system should meet [R42]([R42]PHI should
be anonymized when possible). In the case of interfacing with semi-trusted systems, [R40] [Identifying information must not be disclosed to semi-trusted systems] must be met including identifying information from access requests. To conclude, the core principle of the type of semi-altruistic HIE we describe is that it should meet [R41] [Publishing of PHI must be privacy preserving], in that is never discloses additional information either directly or how that data is stored, accessed, aggregated, or otherwise used.

5.3.2 HIE Access Control

The dominant requirement for the AC model is [R12] [The AC scheme must be sufficiently expressive to allow data owners to express privacy policy without compromise]. Data owners must be able to express privacy policy in enough detail to meet their needs. User feedback is required to measure the effectiveness of the AC model in this regard. CAC addresses this by incorporating all the attributes discussed in the corpus as well as being extensible once feedback becomes available.

Static attributes, from an AC perspective, are defined as any attribute which can be evaluated at the time the policy is written and are deterministic in nature. We can be certain if a given user will be granted access to a given datum if all the privacy policy regarding that user and datum are formed using only static attributes. [R13] [Should allow differentiation of PHI by sensitivity], [R14] [Should allow differentiation of PHI by user defined contextual groupings], and [R16] [Should maintain data provenance] are static elements of an AC system. If privacy policy is created with only static attributes we can determine which actors have access to which data until that policy is changed.

[R15] [Should allow access to PHI based on dynamically sensed criteria] requires a second classification of attributes, dynamic attributes. Dynamic attributes are not determined when policy is written, but when the access request made. Contextual factors such as time, locations, state of emergency, and access purpose or workflow required by [R30] [Purpose of use of data should be included with access requests] are dynamic attributes. It is possible to meet [R23] [Should allow for persistent and ephemeral contextual groups of actors] by allowing actors to be constrained by a temporal dynamic attribute. Similarly, a persistent group may be defined by the static member
alias. Evaluating a AC policy using only dynamic attributes would require a probabilistic approach and need to be informed by assumptions, heuristics, and contextual information to provide a reasonable estimate. A policy containing a single dynamic attribute is a dynamic policy.

The goal of PCP systems is not to prevent others from accessing data but to ensure the some form of consent is collected from the owner before data is disclosed. [R28] is integral to achieving this goal. One advantage to [R28] is that is allows data owners time to review their current policy before adapting it to disclose new data. [R28] is incompatible systems which grant default access to administrators or 3rd parties. Conversely, data owners should never be denied access to their data by [R27].

Data owners must be able to share PHI with care providers. Not every system which stores PHI needs to facilitate sharing, however, from the corpus it is clear there is a significant advantage to doing so. We will focus on PHI sharing systems as simple storage would be a subset of the identified requirements and much simpler to implement. We must assume then that that any AC in such an eHealth system would be required to satisfy [R29].

According to price the circle of care extends beyond formal care providers we establish [R21] to differentiate formal care providers from friends and family who may be involved in the treatment of the subject of care. A patient may not know every care provider at a care facility to have some level of trust with all providers at that facility, as with hospitals. Lay people may also be associated to a data owner through an organization such as support groups. Data owners may relate to a single care provider through multiple groups or organizations at the same time. Thus, as with CoHBAC, the actors in the model may represent an individual or group by [R22].

This also allows for data owners to develop trust with individual even when they do not trust the organization that individual belongs to.

The operations performed on the AC need to be verifiable [R18], accountable [R19], and immutable [R20]. In CoHBAC these operations are graph transfor-
mations. Using graph based systems simplifies confirmation of these properties through use of graph tests and secure graph transformations. The intention of these requirements is similar to the ACID set of properties for database transactions. That is, to guarantee validity even in the event of errors, power failures, etc. and provide accountability for after the fact audits.

There are few requirements defining the nature of the PHI itself while there are many requirements built around ensuring that stored PHI can be verified. This is partly due to the fact that there is a large variety of PHI. In this way the PCP framework can be specialized for working with specific types of PHI or in specific formats. The one requirement that directly relates to stored data is [R17](Should allow PHI to be compositional). [R17] is extremely generalized and has a very limited impact on the nature of the stored. However, compositional data is key to providing fine grain AC. Such as in CoHBAC, storing compositional data it is possible to define more restrictive policy on nested PHI and create a hierarchical access structure. This has many user in eHealth such a separation of duties or minimizing disclosure of more sensitive PHI while still providing care providers enough to make informed clinical decisions.

### 5.3.3 Guardians and Custodians

There exists two special cases of users which are important to discuss in a healthcare context: custodians and guardians. Data custodians are individuals or groups who are empowered in addition to the data owner to act on PHI. Guardians are individuals or groups who are empowered by a third party to to act on PHI instead of the data owner.

In the case of custodians, the original data owner is still a present decision making actor in the system. They may be capable of independent choices or be advised by the custodian. The data owner may be able to decide the degree to which a custodian is able to act on their behalf, by [R25](Data custodians may be granted all, or some, of the abilities of a data owner).

A known problem is HIT is data owners exposing their credentials to friends or family acting as custodians. This may take many forms such as granting access to a legitimately authenticated client or exposing credentials to allow the custodian to act unsupervised. Formalizing the role of custodian helps improve security by reducing unnecessary exposure of data owners credentials.
Additionally, accurate data provenance may be useful to clinical decision making if a care provider is reviewing such PHI without context.

Guardians act in lieu of data owners. Most underage citizens are cared for by their biological guardians or through some governmental organization. This is obviously because children are unable to make informed decisions about their health. In many jurisdictions guardians can be legally assigned to those of age if they are unable to make informed decisions, possibly from a developmental disorder, injury incurred by accident, or natural decline in health. While the specific conditions as to what ages and factors play into requiring a legal guardian differ depending on jurisdiction [R24][[R24]Data owners need to be able to have a designated guardian of PHI] must be met, at a minimum, for children. Identity, by [R22], is not bound to representing an individual. And while guardianship implies decision making power, it does not preclude that the subject of cares wishes may be considered of that they retain some limited amount of decision making power in the case of a guardian assigned later in life. To be able to meet these complex health and legal scenarios as they arise, PCAC is designed to meet [R26][[R26]PHI may have more than one owner].

5.3.4 Information Accountability

One of the core responsibilities assigned to the HIE is to manage a reasonable form of risk mitigation by [R43][[R43]PHI systems require reasonable risk mitigation]. Information accountability systems are one way which risk from internal attackers may be mitigated. There are some privacy schemes which circumvent the need for an information accountability authority, [R47][[R47]Distributed public audit schemes can substitute centralized audit services]. These techniques likely arent mature enough to be relied on alone and should be used in conjunction with other techniques for now. Policy aware access logs, [R44][[R44]Should keep policy aware access request logs], are a simple but effective way to ensure information accountability and act as a deterrent for improper legitimate use by [R46][[R46]Should have a deterrent, such as penalties, for improper use] when combined with some disincentives. If users are aware that actions are being recorded, [R45][[R45]Need to clearly communicate that actions are being recorded], reliable logs and a sufficient deterrent reduce threat from internal attackers.
Even when using the aforementioned information accountability techniques, they are only successful if the improper use or malicious attacks are noticed. Keeping logs is not sufficient to catch intruders, they must also be monitored. Later we will discuss empowering data owners, who should be experts in identifying privacy breaches to their own privacy. The HIE is intended primarily to ensure that care providers and data owners can access the data in a timely manner to provide care. And there is a case that any generalized policy could produce an unacceptable number of false positives. With that said there are some minimal techniques, such as patterns in location of access, that can be identified as suspicious activity. So the HIE needs to a minimum monitor the logs to enforce deterrents but also to meet \([\text{R38}]([\text{R48}]\text{Should be monitored to identify suspicious activity})\).

5.3.5 Transparency

Transparency is heavily related to accountability. For the HIE to be trustworthy from an end user perspective it should disclose how it works, \([\text{R36}]([\text{R36}]\text{Need to disclose how data owners policies are enforced})\) which opens the HIE itself to independent audit. In the case that PHI data is lost in a breach, for any reason, it is imperative that the data owner be notified in a timely manner, \([\text{R49}]([\text{R49}]\text{Data owners need be given timely notification of data breaches})\), to prevent further personal damages. While transparency is generally a positive, these eHealth systems must ensure that anything published is privacy preserving. This can include access requests that are not granted. Generally, not having access to some data should appear identical to that data never having existed, from the restricted party's viewpoint, or \([\text{R31}]([\text{R31}]\text{Request makers should not be aware when access is withheld or to what extent it is withheld})\). This is because there is potential social backlash to information being withheld. This problem is more complicated in the case of revoking previously legitimate access, but that was not addressed thoroughly in the corpus.

5.3.6 Consent

Like many of the issues discussed in health care, Consent Precedence, is strongly influenced by the legal, ethical, social, and religious framework it is applied. Universally, \([\text{R32}]\) is seen as a great advantage of networked systems, allowing
care providers to have access to potentially life saving information in a timely manner. How this is to be accomplished and addressing the security concerns is still an open problem in HIT. To provide these life saving services consent systems need to be accessible to a large enough population, [R59]([R59]Consent systems need to be accessible).

Consent can be modeled as three levels which require progressively more informed decision makers and should be more difficult to overturn. Implicit consent is the least binding form of consent, consent drawn from actions, or lack thereof. This is relevant to emergency directives and technology assisting it. Implicit consent is typically enough for non-invasive procedures. A patient visiting a physician is an example of this. By making and attending an appointment the patient has implicitly consented to routine procedures without the doctor needing to explicitly ask permission for every action. Explicit consent requires a patient to expressly agree before the action is taken. Explicit consent is very common in health care, and typically is collected before any actions which might make a patient uncomfortable, this may change depending on the trust relationship and familiarity between care provider and patient. Many eHealth tools gather a form of blanket explicit consent by requiring users agree to a terms of use. Lastly, there is informed consent. Informed consent is not typically collected in health care because of the complexity of the topics and limit resources available to teach or explain them to patients, who are often laypeople. Most health care organizations lack the resources to commit care providers to explain, in detail, every procedure to a patient before performing them. It is not impossible to collect informed consent in health care, any care provider who is also a patient may be informed and specialists and preoperative consultations attempt to help their patients understand the procedures and relation to their condition. eHealth tools also may substantially improve the ability to collect informed consent by providing autonomous educational materials that patients can review and understand at their own rate without using human resources. There is an open debate in many jurisdictions and domains about the responsibility of service providers to ensure that users understand the terms of use before they are able to agree to certain activities. To address this problem [R33] ([R33]May provide a mechanism to overturn explicit consent to provide care to that individual) and [R34] ([R34]Should not provide a mechanism to overturn informed consent to provide care to that individual) indicate
that explicit consent may be overturned by a more informed individual working in the patients best interest and that informed consent should not. The exception to this rule is that one patients privacy should not adversely affect another patients health. And while it can be difficult to detect, regulate, and enforce such conflicts if a system is capable it should do just that by [R35]([R35]Should provide a mechanism to overturn consent to provide care to another individual).

The issue still remains that while we may classify types of consent the most important aspect it ensure that the consent, and repercussions of giving it, are understood by the patient in question. It is difficult to define how an eHealth system may meet [R58]([R58]Consent systems need to be understandable) and it may depend greatly on the legal framework in which the question is asked. As many eHealth systems dont require more than implicit or minimal explicit consent to perform their purpose this issue only becomes truly challenging as the need to collect informed consent rises.

5.4 Client

Up until this point we have discussed the infrastructure to facilitate PCP systems. Now we will examine how end users, including, data owners, interact directly with the system and define policy, through clients. A single eHealth system may have one client or many clients. As the focus of this work is patient centered privacy we will forgo a discussion about administrative or provider centered clients.

The specific design of an interface to deliver all the discussed controls for patients and data owners is not covered extensively in the corpus. However, we put forward [R64]([R64]PHI management tools need to lead data owners to make rational decisions) as one of the primary goals of an eHealth tools interface based on the assumptions and contexts of the studies reviewed. Identifying how eHealth tools clients may accomplish this will require a body of work of its own and will be discussed in future work.

5.4.1 New Users

Data owners may have an eHealth system brought to their attention in many ways depending on the nature of the service and its provider. Many systems
rly on end users to make first contact and rely on traditional advertising methods to reach their intended markets. Attracting and keeping users is a major consideration when attempting to build social networks and profitable business. However, we leave the specifics of the competing service marketplace to future work and contribute to them by identifying how we can raise systemic trust through the service provided. We will assume patients can use the eHealth systems discussed to help meet some health goals, social or otherwise, and that will create a user population regardless of market conditions.

Once a potential user is aware of a service and has intention to use it they require a client. Typical clients come directly from service providers and deny any use without agreeing to terms of service beforehand. Other models, such as those using providing API services, assume multiple third party clients may be available. For the purpose of this work will assume that it is trivial for data owners to locate a trustworthy client and that all clients form some contract with the service provider by interfacing. There has been significant debate over the content of terms of service and its need to be accessible to those who agree to them. While this can change from one legislative framework to the next, it is generally agreed that data owners have the right to decide when there data is collected, used, or disclosed and may choose to waive those rights. Data owners need to be sufficiently informed when their data is collected, used, disclosed, or aggregated) further requires that data owners be informed when their data is being used in aggregations, although not all data owners may be able to understand the risks associated with data aggregation.

There is a standing question of how best, and if it is reasonably possible, to educate data owners, including laypeople, on the risks and countermeasures in eHealth systems. As mentioned previously, the broad populations which may derive benefit from eHealth systems implies a variety of skill levels and individual capabilities. CoHBAC, and its successor Privacy Centered Access Control (PCAC) which will be presented later in this work, attempt to address this from a conceptual standpoint by creating a connections between the contextual experience the patient is having, such as an illness, side effect, or on going treatment, and the policy itself. This population does not preclude the other extremes, informed data owners who have specific wants/needs for their data privacy and the capability to implement them. For this reason, and many others, it has be repeatedly suggested that a single eHealth system may require
multiple client interfaces to address the user skill gap. [R61](Educate data owners on risks of misuse of legitimate access) begins to address minimum required user education by describing the responsibility to ensure that every user understand the need for secrecy of authentication credentials. Malicious users who obtain legitimate credentials undermine the basis for many of the risk mitigation techniques discussed. Accountability may be assigned to the owner of the alias misused but the damage cannot be directly undone. Furthermore, even if all access is legitimate and honest but curious insiders are sufficiently deterred or accountable there still exists a non-zero risk that the system may be compromised by a malicious attacker through physical or electronic means. In recognizing this possibility [R62](Educate data owners on risks breach and how to minimize damage) is put forward, although there may be no meaningful way to mitigate damage, depending on the type of PHI disclosed, by acknowledging the possibility of such an event data owners may be empowered to claim ownership of their PHI beyond the single eHealth system in which it is contained. Together, [R61] and [R62], form a meaningful minimum skill level for maintain PHI privacy, even if the user does not understand the mechanism. We leave measuring if a user is sufficiently educated for further discussion in future work.

We refer to users of a system who are skilled in both the specific workings of that system as well as the platform on which the client is presented as power users. In this regard, eHealth systems are analogous to popular operating systems, such as the Windows platform, in which a simplified (graphical) interface is sufficient for the needs of the average user but tools are included for more direct manipulation of the software. In eHealth systems power users who are data owners may want to express specific policy for their PHI and have the cognitive skills to maintain complex policy over a long period of time. These users would be expected not to trust, or use, an eHealth system that did not sufficiently meet their privacy needs. For a small eHealth system this would be a minimal loss, and likely the system provides an comparatively small benefit to health outcomes. For larger eHealth systems, those large enough to gain benefit from population health analysis, the loss of these power users would have many negative effects. First, as power users are data owners themselves and possess PHI which may aid in the population health analysis, furthermore, the loss of a whole demographic may impact or bias analysis. Secondly, as the system
grows larger it represents a larger attack surface and obtaining trust becomes more difficult from informed users. Increasing the transparency of such a system, that is, informing users about how data is stored, managed, and accessed as well as what what countermeasures are in place, [R51][R51](Data owners should be sufficiently informed of how PHI is stored, managed, and accessed) and [R63][R63](Inform data owners what preventative measures and risk mitigation techniques are actively implemented), opens those systems to independent audit by those same power users who have a motivation to ensure that their data is being protected the way it is claimed. Ultimately, it is not only users with existing skills who would take advantage of the transparency, any user may be able to learn enough about the specific system to overcome difficulties with the platform if sufficiently motivated. Thus, an honest system which opens itself to this kind of auditability stands to gain user trust directly and second hand through the reputation and recommendation of satisfied auditors.

We have established, and built into the AC model, access logs are a necessary part of maintaining PHI privacy. [R57][R57](Access logs need to be presented to data owners in a user friendly manner) allows individual data to be audited as opposed to the system which stores it. Although we leave discussion of what a user friendly manner is to future work, we suggest that because access logs relate only to the PHI, users, and context of the data owner that they are the best authority to perform the audit. [R51] and [R63] may not be sufficient to build trust in an eHealth although they contribute to trust of the logs themselves. [R57] ensures that if every user were empowered to do so they would have the ability to reliably audit their PHI.

5.4.2 Access to Stored Information

After a user creates an alias and agrees to the terms of a service the next step is to generate or import PHI. In many cases, the information stored in the identity is sufficiently identifying to be PHI itself. This is one of the reasons the terms of service are so vital during the initialization. With regards to the composition and structure of stored PHI, we defer to the AC model. It is important to note that an interface may not provide all the functionality allowed by the AC model. This allows for a system with a simplified interface which lacks many potential controls supported by the model but which satisfies users with weaker technical
or cognitive skills. [R55] Data owners may require a simplified interface) is weakly worded because this need may only be identified within the context of a specific eHealth tool and the PHI it protects; an extremely simple system may be unable to simply the interface any further. [R52] Must provide a reasonably manageable access control interface for data owners) attempts to address the concern that an interface may not provide vital functionality supported by the AC model. We leave interpretation of reasonable intentionally ambiguous but we define the intention of the AC control scheme rigorously by [R12] The AC scheme must be sufficiently expressive to allow data owners to express privacy policy without compromise). An argument can be made that if an eHealth system were bound to meet the combination of [R52] and [R12] without reasonable limitations that some honest or malicious actor could demand a level of expressiveness which is prohibitively costly to provide. We leave the discussion of this extreme as future work. To accomplish these usability goals the interface should also allow data owners to satisfy [R53] Data owners need to be able to enforce new AC policy in real-time). That is not to imply that every action must be instantly committed, but that no unnecessary bureaucracy is required for data owners to quickly and efficiently change privacy policy.

With regards to the interface design we propose [R54] AC interfaces must be intuitive). At a basic level we define intuitiveness as a measure that the provided functions be reasonably usable and physically present and accessible. Data owners also need to be engaged by these tools by [R56] Data owners need to be engaged with their privacy tools), engagement and intuitiveness are further discussed in future work as both are difficult to measure and subjective to a given users preferences. While we cannot present a comprehensive definition of user engagement at this time, we tend to correlate it with the perceived value the user is returned for their investment in using a tool. In the health care domain, engaging users can be analogous to informing and educating users sufficiently to understand the health benefits to using the tools and valuing it enough to be worth using, even with the additional cognitive load.
5.4.3 Mobile Clients and Sensors

As mobile computers and sensors improve so to does the ability to sense and deliver data directly to and from the data owner in real-time. There is a large body of work on the effects of alert fatigue and its negative impact, potentially causing critical alerts to be overlooked. [R60][R60]Data owners may subscribe to alerts relevant to managing PHI) needs further study to refine but there is undoubtedly value to receiving timely alerts about PHI. This may be in the form of an emergency response scheme or alerting of unauthorized PHI access. The nature and usefulness of alerts needs to be further studied in the context of specific PHI an eHealth tools.

Mobile sensors may also generate PHI. This has been discussed in terms of dynamic attributes for AC policy. This is a relatively new field, especially in the preventive health space. Future work will uncover the pros and cons of use, for now, we state that by [R65][R65]Sensors data requires high integrity) the integrity of these sensors needs to be ensured if clinical decisions are to be based off them. If there are significant risks to integrity there may be need to a user education about the risks.

This concludes discussion of the PCP Framework, its components, and related requirements. To further demonstrate the applicability of our framework and the viability of meeting the requirements, in the next chapter we present the design of an eHealth system which adheres to the requirements described by the PCP framework. For reference we name this hypothetical system CanCare.
Chapter 6

Applying the Patient Centered Privacy Framework

6.1 CanCare: A Privacy Centered eHealth System

We present CanCare as the vision of an eHealth system that is independent, but regulated, by the Canadian government. The goal is to design a system which will allow secure storage of clinical PHI by demonstrating the ability to meet all the identified requirements simultaneously. CanCare will fill all the roles of a PCP system. It is empowered to act independently from the government itself so it fills the role of TSP by directly engaging with data owners. CanCare will be provided the resources to own and maintain a sufficiently large data center allowing it to directly manage storage. CanCare will also have an in house development team including any required specialists such as security experts. This development team will maintain the infrastructure, including ongoing preventative security and internal tools to maintain the HIE. CanCare will also develop the end user clients; for data owners this is limited to a browser based tool, for clinicians this includes interoperability with other clinical tools and alert based systems which require a mobile client.
6.1.1 Trusted Service Provider

CanCare, as TSP, can employ traditional authentication protocols such as challenge-handshake authentication protocols allowing us to meet [R1](Connection requests must be reasonable authenticated). With access to government issued identification records as well as clinical and business licences CanCare should be able to reasonably determine the identity of any single actor or group of actors meeting [R3](Must establish a secure communication channel with any actor). Government issue identification is a fairly transparent process and the nature of challenge-handshake protocols, and the subsequent password authentication protocols which can be established, are easily verifiable to an informed user to meet [R2](Should disclose authentication process). Ideally, these requirements would be auditable by any user, however, we do not possess an adequate way in the scope of this research to educate and inform lay people about network security. It is assumed that a sufficiently invested individual could perform the audit or an independent expert could be hired for the task.

6.1.2 Storage

The PHI stored by CanCare is not edited while it is stored. While some limited ability to add metadata, such as providence, access logs, and notes is provided, only clinical PHI is allowed from registered care providers. CanCare allows other eHealth tools to upload PHI. Uploaded PHI is wholly owned by the data owner or their guardian once transmitted. Consent to upload this data must be gathered. Physical or electronic signatures are required at the point of care. Data requests may only be made groups and practises which are approved and from approved eHealth platforms. CanCare will develop and maintain the intraoperative framework to send and receive data from other eHealth systems and can discontinue support if needed. As a TSP, CanCare meets [R5](Must avoid integrating with untrusted systems) through their control of the storage medium and ability to adjust if any user group or eHealth platform is compromised.

CanCare will own and operate a single central data center which will service all of Canada. Given that CanCare employs skilled developers to manage said warehouse it is trivial to provide reasonable network security for [R11](Reasonable network(external) security is required for storage of PHI). Furthermore, by generating checksums to confirm data integrity we meet [R4](Must have a mech-
anism to verify the integrity of stored and retrieved data). In this way we also meet [R8]([R8]Should serve unaltered stored PHI) as our storage is directly managed by the TSP and any storage or retrieval errors should be detectable by using the checksum. All PHI is backed up and recoverable using standard data warehousing techniques to meet [R10]([R10]PHI must be backed up and recoverable). The data centre itself should be outfitted with backup power generator and supplies sufficient to provide assurances for accessibility by [R6]Must grant access to PHI in a timely manner. As we are not limited in resources we can assume sufficient computing power to store only encrypted data to meet [R9]([R9]Should not have access to unencrypted PHI) and the ability to requisition more as needed to meet [R7]([R7]PHI storage must be scalable). With enough resources it is possible to meet scalability goals with relatively simple encryption schemes. However, a large body of work exists to find more efficient and scalable way to store and access encrypted data in a privacy preserving manner and can be employed to reduce costs. These techniques are not necessary to meet the PCP requirements but are not detrimental either.

### 6.1.3 Health Information Exchange

**Information Security**

CanCare develops and maintains its own servers and clients which allows it to act as the HIE. The HIE must maintain reasonable security based on the aforementioned authentication scheme. We suggest that the specific scheme chosen is trivial but that CanCare will possesses developers capable of ongoing security development more indicative of its ability to meet [R39]([R39]PHI requires sufficient cryptography). For completeness will state that CanCare uses some form of symmetric encryption using government issue intensifiers and only provides clients that connect through the HTTPS protocol. CanCare has reasonable vetting/authentication and encryption schemes and by directly managing all parts of the PCP framework can meet [R40]([R40]Identifying information must not be disclosed to untrusted systems)

While CanCare is not limited by resources it is still worth mentioning that the chosen security scheme must be reasonably efficient as described by [R38]([R38]Consent schemes must be efficient enough to not impact availability). Efficiency is important because functionality, such as revoking privileges, may be difficult to
implement with some kinds of encryption. This topic was frequently covered by literature which did not pass our inclusion criteria. Revoking privileges is one of these problems. CanCare allows data owners to revoke privileges and we assume with sufficient resources that CanCare meets \([R37]\) ([R37] Patients need to be able to revoke access) and \([R38]\) regardless of the implementation. As previously mentioned, CanCare continuously develops its security and will given time will eventually implement the most efficient algorithm which is privacy preserving.

**Access Control**

The CanCare HIE implements the instance of PCAC modeled in figure 6.1. PCAC is intended to be extensible and may have more attributes or data types if needed. Extensibility allows PCAC to satisfy \([R12]\) ([R12] The AC scheme must be sufficiently expressive to allow data owners to express privacy policy without compromise). Only through significant review of user feedback and over time can any eHealth system determine to what degree they are able to satisfy the user population. We cannot predict those needs but we believe from our review of the literature that PCAC has the ability to represent any privacy policy needed.

In figure 6.1 PHI is structured with a reflexive relationship to allow composition and segregation of data by \([R17]\) ([R17] Should allow PHI to be compositional). Stored PHI and actor groups are constrained by a shared set of attributes. The specific attributes required depend on the nature of stored PHI and the needs of the data owners. As demonstrated by CoHBAC we can meet the following requirements by defining appropriate attributes: \([R13]\) ([R13] Should allow differentiation of PHI by sensitivity) by including a sensitivity attribute allowing differentiation by policy of otherwise similar data; \([R14]\) ([R14] Should allow differentiation of PHI by user defined contextual groupings) by allowing user generate context labels. These labels should be unique and may also be generated when actor groups are constructed; \([R16]\) ([R16] Should maintain data provenance) by adding the appropriate attribute. In this way attributes may also function as meta data to some degree. We further add \([R15]\) ([R15] Should allow access to PHI based on dynamically sensed criteria) and the related attribute type to encapsulate policy relevant sensed data.
The actor model in PCAC follows closely to CoHBAC. CanCare allows groups or individuals to be represented by a single alias meeting [R21](R22)Actors should be able to represent an individual or entire organizations or groups). As discussed with the authentication scheme, it is possible to extend the information stored in the alias to provide registered care providers as well as lay people by [R21](R21)Individual actors may be licensed care providers or trusted lay people), although formal caregiver may require additional scrutiny of identification. And as groups are constrained by the same attributes as data, we expand [R15] to include temporal attributes which allows access to be defined as persistent or ephemeral by [R23](R23)Should allow for persistent and ephemeral contextual groups of actors).

PCAC supports custodians and guardians as actor types by default which meets [R24](R24)Data owners need to be able to have a designated guardian of PHI). Moreover, we define guardians as a type of owner as they are typically equivalent to a data owner and empowered by law. Guardians may not be the sole owner of data even if they are the only owner capable of affecting policy.
Such is the case with children, their parents act as guardian of their PHI until they come of age. To address the difficult legal situations this can lead to we allow for data to have multiple owners, provided all owners other than the subject of care are guardians, this meets \([R26](\text{PHI may have more than one owner})\)

We define custodians as a type of actor as they are empowered by data owners and the data owners maintain the right to redefine or revoke those privileges. To simplify management we allow users to define policy which includes editing rights on actor groups and PHI. This allows data owners to create groups which only allow custodians and those groups to be granted some amount of the viewing and editing powers of a data owner, meeting \([R25](\text{Data custodians may be granted all, or some, of the abilities of a data owner})\). There is one caveat, that a non-data owner may not edit a data owners permissions which allows us to meet \([R27](\text{Must grant data owners access to PHI when requested})\). This allows for complex situations involving multiple data owners without allowing for lateral privilege escalation by custodians. Multiple owner situations need to be informed by a specific legislative context so we will not discuss them further in the scope of this work.

**Access Control Model Transformations**

Like its predecessor, PCAC is a graph based AC model. One way of specifying a secure AC model is to define a secure initial state and a set of secure transformations that are guaranteed to output a secure system state given that their input is a secure system state. We define the initial state of our AC graph as the empty graph, which, obviously can be considered secure, as it provides no privileges. Therefore we can meet \([R28](\text{Access should be restricted to the data owner by default})\). CanCare will maintain the minimum required set of secure transformations. Required operations include: Add relationship, Delete relationship, Create Group, Delete Group, Add group member, Remove group member, Add data, Remove data, Create policy, Delete policy. Each operation defined this way is verifiable and immutable, \([R18](\text{Each operation to PHI should be verifiable})\) and \([R20](\text{Each operation to PHI should be immutable})\). We further add that each operation must be recorded as an atomic part of the operation to meet \([R19](\text{Each operation to PHI should})\)
be accountable).

**Access Requests and Graph Tests**

If the security state is according to the above graph model, we can precisely define AC decisions using graph tests. Graph tests evaluate to true if access should be granted and to FALSE otherwise. We can use PCAC and graph tests to assess whether access should be granted for a given access request. Requests may be have their purpose explicitly, however, CanCare will assume purpose of use related to the group the actor makes the request through. When an access request may be granted through more than one group the request maker must explicitly choose the most relevant group to be recorded with the request. In this way we address [R30](Purpose of use of data should be included with access requests).

The policy defined determines the specific relationship between data and actors but at a minimum it must allow data owners to define viewing rights to their data by [R29](Data owners need to be able to authorize others to access PHI). Authentic data owners, by definition, have the ability to view any data they own. Since data owners must have access any disclosure to them will be privacy preserving. To meet [R41](Publishing of PHI must be privacy preserving) for legitimate access CanCare must guarantee that AC policy is enforced as written, which it can do through by being transparent in the form of policy aware access logs. There is also an external element to [R41] in that meta data, PCAC attributes, also must not reveal any additional information about the owner of the PHI. Meta data such as access logs can reveal identifying information about the owner or PHI itself. For example, if actor was unable to access a specific PHI but could see that it had been accessed recently by a known oncologist they may infer the nature of the illness disclosed in the PHI. While there are other similar examples of non-privacy preserving PHI publishing, such as ineffective anonymization, we leave in-depth investigation into that as future work. However, it is clear from the corpus that knowledge that the fact that access has been denied is in itself meta data, the requester now knows that PHI exists which they cannot access. To address this and [R31](Request makers should not be aware when access is withheld or to what extent it is withheld) the CanCare HIE response to a denied access request
should be indistinguishable from the response for a datum that does not exist.

**Consent Precedence**

Emergency access to PHI leads to better decision making for first responders and other emergency care providers. However, it is clear that unrestricted access to PHI has, to some users, an equivalent amount of danger. To reconcile this opposing views, CanCare implements two predefined groups for every new data owner: NewProvider and Emergency. Both groups start empty. All new data owners are presented with the option during onboarding to make demographic information (name, age, etc.) available in case of emergency. A provider facing companion application to access this information is outside the scope of this description, however, it is self-evident the value it presents if properly, and securely, implemented which meets [R32]([R32]Should provide a mechanism to overturn implicit consent to provide care to that individual(break-the-glass)). Data owners may add other actors and PHI to the Emergency and NewProvider groups as needed and an emergency actor may be placed in that group as to ensure the any operations that actor preforms are captured and accountable.

CanCare does not extend any additional emergency powers or mechanisms to overturn consent, meeting [R34]([R34]Should not provide a mechanism to overturn informed consent to provide care to that individual). Since not all patients have access to privacy controls at the point of care, CanCare allows providers to collect a signature as consent to add themselves to that patients NewProvider group. Signed documents are a form of explicit consent and no other mechanism exists to satisfy [R33]([R33]May provide a mechanism to overturn explicit consent to provide care to that individual). [R35]([R35]Should provide a mechanism to overturn consent to provide care to another individual) is applicable in complex health scenarios which require further investigation. We will not go into the legal background of these scenarios. An example of a complex health scenario and how CanCare might adapt to address it as follows. Contagious diseases such as, Ebola, are often under observation by health authorities. Travel advisories, vaccination, or return screening may be among best practises for minimizing risk of exposure. The knowledge of who has travelled or is travelling to those locations becomes valuable PHI to government, travel, and health stakeholders. CanCare, if empowered by legislation, would
be in a position to collect and distribute that PHI from the travel sector to the appropriate care providers.

**Information Accountability**

The CanCare HIE maintains information accountability through policy aware logs. Access requests made are recorded both in the HIE itself and with the PHI it requested which should be sufficient to meet [R44]([R44]Should keep policy aware access request logs). All employees of CanCare are educated that they are being recorded and there is a zero tolerance policy for unauthorized access of PHI, [R46]([R46]Should have a deterrent, such as penalties, for improper use). All users are reminded they are being recorded every time they authenticate. By meeting [R45]([R45]Need to clearly communicate that actions are being recorded) and [R46] we minimize the threat from internal honest-but-curious actors.

CanCare keeps all stored PHI anonymized at all times by [R42]([R42]PHI should be anonymized when possible). Well recorded internal records and anonymized data protected against physical theft should be sufficiently audit-able and no public audit scheme will be implemented, [R47]([R47]Distributed public audit schemes can substitute centralized audit services)

Any member of the public will be able to access a description of the CanCare architecture. This publicly available information will be as detailed as it can be without compromising security. This allows interested parties to access the security state themselves and satisfies [R36]([R36]Need to disclose how data owners policies are enforced).

Generally CanCare will make no attempt to relate access requests to identity. However, in the interest of patient safety, data owners will be informed if a data request is made from out of country. In these cases, disclosure of PHI would also change jurisdiction. As of this writing Canadian eHealth systems cannot send and PHI out of the country and it is likely CanCare would be required to comply to that as well. We believe these factors contribute to reasonably satisfying [R48]([R48]Should be monitored to identify suspicious activity) without interfering with legitimate access.

A breach may be found to occur, or is highly likely to have occurred, and be detected by the security engineers. The CanCare policy is immediately
informing all affected users and continuous updates with as much detail as can be given without impacting an ongoing investigation. This policy satisfies [R49](Data owners need be given timely notification of data breaches).

Through the combined efforts of all of the above techniques and the inherent design of PCP systems we believe CanCare reasonably attempts to mitigate risk,[R43](PHI systems require reasonable risk mitigation), as well as minimize damages should they occur.

6.1.4 Clients

CanCare provides its own in-house developed clients to interface with the HIE. We have no provided mock-up or prototypes at this time. Several prototypes exist for CoHBAC, however, they lack significant user testing and validation. We will describe some features and how we envision navigation but the published client needs to be the result of many iterations of user feedback and is beyond the scope of this work. Similarly, we describe where we might educate a user or inform them but most known user education techniques are not completely effective e.g. alerts allow delivery of PHI to the point of care but too many alerts leads to alert fatigue and the content may not be delivered effectively. We will discuss in future work more detailed investigation of the relationship between clients and users.

Recruitment

In our context, CanCare will only be accessible through the internet by standard browser. This limits accessibility somewhat, however, due to the additional challenge of delivering all the needs of PCP in a mobile interface it may require a significant amount of additional research to be reasonably secure. To meet [R65](Sensors data requires high integrity) we would need reliable sensors to leverage new technology which may need to be reviewed on a case by case basis. We will discuss dynamic attributes and sensors more in future work as there is an established field and definition of medical devices and substantial legislation as well.

All new users will have to establish their alias and credentials before any progression. First time users are presented with a simplified description that their data is not used or disclosed while it is stored in CanCare and is only shared
by their authorization; meeting [R50][R50]Data owners need to be sufficiently informed when their data is collected, used, disclosed, or aggregated) provided all future disclosures require consent as described by the AC model.

New users will also be explicitly warned about the dangerous of lost, disclosed, or shared credentials by [R61][R61]Educate data owners on risks of misuse of legitimate access). At this time they will also be shown where they can change their credentials and informed they should do so if they ever suspect their account has been compromised, [R62][R62]Educate data owners on risks breach and how to minimize damage).

New users will also be shown where they can access more information. As discussed with [R36][R36]Need to disclose how data owners policies are enforced), CanCare is transparent in that it makes available all information about the operation and management of the CanCare system which does not compromise security, this will allow us to meet [R51][R51]Data owners should be sufficiently informed of how PHI is stored, managed, and accessed) and [R63][R63]Inform data owners what preventative measures and risk mitigation techniques are actively implemented).

**Workflow Aware Access**

There are three core work flows in the CanCare system, excluding those used for creating and maintaining accounts: Creating groups and associating actors with groups. This includes finding and associating with new actors; Storing, viewing, and curating groups of PHI; Associating groups of actors with groups of PHI. Each of these work flows needs to have its own interface, and furthermore, CanCare provides a simplified version of each with only the minimal necessary information to meet [R55]Data owners may require a simplified interface. Only significant user testing can establish if the interfaces are intuitive [R54]AC interfaces must be intuitive) or understandable [R58]Consent systems need to be understandable). Separating the interface into actors, data, and relationships we hope to introduce these features by design. Accessibility features may be provided as well. Support for the visually or hearing impaired is a well established field of interface design. Furthermore, by providing simplified interfaces CanCare is also accessible to the cognitively impaired. Additional language and character set support may also contribute to accessibility and in
the Canadian government context it can be assumed that both English and French language support are required. Combined we create a basis of accessibility [R59](Consent systems need to be accessible).

Access logs need to be provided in a user friendly format by [R57](Access logs need to be presented to data owners in a user friendly manner). We propose to display access logs in two ways. First, a master list of all access with three attributes: datetime, requester alias, requester group (recall requests are made through single group even when multiple may be used). Secondly, each PHI has its access recorded and can be reviewed for each individual piece of PHI and collection of. The CanCare client allows data owners to opt in to receive alerts through email or SMS. Actor groups, PHI, and policies may be flagged for alerts whenever they are active, [R60](Data owners may subscribe to alerts relevant to managing PHI).

The relationship interface allows data owners to directly describe and review their AC policy and satisfy [R52](Must provide a reasonably manageable access control interface for data owners). Through this interface, authenticated user may implement changes to privacy policy which will be propagated to the HIE in real-time, [R53](Data owners need to be able to enforce new AC policy in real-time). By allowing data owners to have a tangible impact on their privacy we hope to engage all privacy conscious users and meet [R56](Data owners need to be engaged with their privacy tools).

The ultimate goal of the CanCare client is to meet [R64](PHI management tools need to lead data owners to make rational decisions). It is extremely difficult to precisely define rationality in terms of privacy, partially because of the variety and individuality of each data owners privacy needs. Therefore user feedback is an integral part meeting this goal. We describe how an interface might meet user needs and incorporate feedback but are aware that at this time we are unable to sufficiently prove we can meet these requirements.

This concludes the CanCare model, a demonstration of a Patient Centered Privacy eHealth system. While we cannot provide complete and total verification without large scale implementation of a system such as CanCare we believe from the reviewed literature that the framework is well informed and flexible enough to adapt to future work, both on the abstract model and instanced implementation.
Chapter 7

Contributions and Implications, Limitations, and Future Work

7.1 Contributions

We initially set out to investigate our research goal which is “What are the requirements of electronic health care systems which place patient health and privacy above all other concerns”. After preliminary review of the literature it was clear that few, if any, complete patient centered privacy systems existed. Of the systems that were implemented they existed in several different jurisdictions, at different times, with different goals making it difficult to compare or even measure their ability to provide to the patient’s needs.

We took a grounded theory approach to the problem. We reasoned it was better to gather a heterogeneous sampling of the state of privacy controls as opposed to an in-depth look at any single legal or social framework. Our first research question was “What is known in the current literature about AC models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility.” In identifying quality sources and gathering and reviewing a significant, and repeatable, corpus we have attempted to establish a shared understand of the domain and associated assumptions. We present this as the summarized review of the literature and more formally in the conceptual model underpinning our framework.

The development of Circle of Health based Access Control was a step towards better defining what patient centered systems will look like. However,
the access control model alone is insufficient to provide any reasonable degree of privacy. To quantify the degree to which eHealth systems deliver patient privacy we identified 65 requirements to satisfy our second research question: “What are the requirements for access control and privacy controls in patient facing health systems with regards to creating comprehensible and maintainable privacy systems.” While we acknowledge that these requirements may not be complete it is a significant achievement in creating a shared understanding of patient privacy for future development.

We organized our findings into the Patient Centered Privacy Framework. This framework aligns the identified requirements with the fundamental need for accountability for patients. The framework acts as a tool to measure existing systems against and aid in the development of future systems. The four components of the framework: the Trusted Service Provider, Health Information Exchange, Storage, and Clients are designed to better identify and discuss how promises and obligations made to patients are upheld and which have failed in the case of a breach or accident. We will discuss future applications and extensions to this framework in future work.

### 7.2 Limitations

We now will address the limitations with our methodology. Firstly, while our literature reviews were informed by controlled vocabulary they were not exhaustive. Only English language publications were reviewed and only those on the Compendex, Inspec, and Pubmed indexing services. As discussed with the methodology, these three databases represent a significant portion of the English publications in this field. As the proposed framework is not intended to be a finished product additional sources may be reviewed and their result further synthesized into the framework and AC model.

An alternative mode of investigation for this research would have been to interview directly the primary users of eHealth care systems such as patients, providers, and developers. This would have provided, however, only a partial view into the problem being studied. While significant amounts of academic literature was reviewed directly engaging primary users may lead to a different perspective and different results. Typically, interviews or questionnaires target groups which share legislative or social frameworks, i.e. respondents are often
from a single country. While there is value to understanding and comparing the differences between these contexts or developing in-depth knowledge of a single context, we believe there is more value to this work in sampling a broad set of literature across many contexts to better identify the core needs of all individuals who may access health services.

The first literature review was performed by two independent reviewers who had to agree on the included corpus. This strengthens that literature review by removing selection bias. The second literature review was only completed by a single reviewer. This is because of the specialized knowledge required to work in the intersection of security and health care domains. To address this issue the literature review was conducted in a repeatable way. If a verification was completed and found to differ significantly, the two resultant reviews could be further synthesized by a third independent review.

There are very few eHealth systems that prioritize patient privacy over economic gain. Creating such a system at scale is a large development. While it is possible to review the individual issues out of context the result of our study shows that it is imperative to consider the entire eHealth system. We present CanCare to show that it is reasonable to design a PCP system which meets all the requirements. Such a system may not be realistic or economically viable, however, demonstrating that a system may meet all the PCP requirements is only the first step to investigate how other systems do not. This ideal system can help identify privacy sacrificing behaviour and its causes.

Not all patients desire privacy for their PHI. In the healthcare population there is guaranteed to be some subset of patients who are privacy conscious. These users would be more inclined to disclose to a system they trust and maintaining their privacy is a way to build trust. By explicitly including simplified interfaces we intend that implementing PCP systems should not be notable different for the average user than a non-PCP system. In this way, even if many or most patient do not value privacy they are not lost or inconvenienced while satisfying those that are. These privacy conscious users, if satisfied, may then help other less technically capable users come to trust the system as well.
7.3 Future work

The most straightforward extension of this work is to continue reviewing literature to address the areas of our model that need improvement. Notably, a significant weakness in our work is in identifying how specifically to design interfaces to communicate universally with data owners. We acknowledge in our work that multiple interfaces may be required but that is only one possible solution and would reasonably expect to be refined through another literature review. Other areas which could benefit from more targeted review are: organizational security, encryption techniques, accessible interfaces, and user education.

For user interface and education, a significant amount of work must be done in user testing to determine if any interface is satisfactory. One approach would be to identify ways to universally improve the quality of eHealth interfaces. Future work into knowability of the PCAC model would help understand better how to educate users and ensure they can write and maintain privacy policy. Alternatively, an existing eHealth system could use user testing to inform changes in their interface to better adhere to the requirements of PCP systems. Subsequent versions of the PCP framework are intended to a scoping set of guidelines for both preventive and proactive development towards providing patient centered privacy.

Often during this work we mentioned that the PCP framework could be instanced to better represent a given jurisdiction with additional requirements described by the relevant legislation. Those instances can then be used to better perform case studies in their respective contexts. Performing case studies on existing or defunct eHealth systems may give further insight into comparing their relative strengths and weaknesses. Furthermore, we could begin to identify if any priority exists among the identified requirements. By applying the PCP framework in various case studies we can discover if successfully systems fulfill similar subsets of the PCP Framework requirements. Following up with primary users of these systems could lead to further insights into their mental model of privacy and any limitations these systems may be able to improve on.

As smart devices and high quality sensors become more widely available there there has been a significant investigation into how they can be used to improve health outcomes. CanCare focused on traditional Electronic Medical Records (EMRs), however, neither the PCP framework or PCAC model are
limited to working on that kind of PHI. Online Social Networks in healthcare are an open problem and there is evidence to suggest that improved support networks lead to improved health outcomes, however, it remains difficult to measure those outcomes. PCP framework may be further expanded to deal with new technology and platforms.

As stated repeatedly, the focus of this work is on subjects of care, not providers or business owners. A companion to this work would be a similar investigation from a provider perspective. There are significantly more provider facing tools than patient facing tools in healthcare. Which means there is a larger body of work to pull from. While it is important to investigate this we believe this problem is related but fundamentally different. This leads to two important areas of interest: how to make provider facing tools facilitate patient controlled systems, and how to make patient facing tools facilitate provider workflows.

7.4 Conclusion

We answered our first research question, which generated Circle of Health Based Access Control (CoHBAC), by investigating what was known in the the literature about Access Control (AC) models for consumer health informatics applications, including their effectiveness, limitations and comprehensibility. Ultimately, the scoping review discovered the current state of patient centered electronic health (eHealth), its limitations, and a variety of approaches in how an AC model could better meet the needs of care providers and subjects of care.

In this work we have investigated what is known about access control and privacy controls in patient centered health systems with regards to creating knowable and maintainable privacy systems. The systematic literature review corpus informed a wider scope for privacy in eHealth systems. Accountability, transparency, and patient consent were dominant requirements which traditional patient facing tools were failing to meet. To create a knowable and maintainable model for patient centered privacy controls we identified requirements to answer our second research question and determined what the requirements are for access control and privacy controls in patient facing health systems with regards to creating comprehensible and maintainable privacy systems. We then organized these requirements into the Patient Centered Privacy (PCP) Framework.
The PCP Framework, and the PCP eHealth systems it describes, envision empowered data owners who are the ultimate authority on the collection, storage, and disclosure of Personal Health Information and provide a standardized way to communicate about the responsibilities of those who secure sensitive information.

In the future we want to see the PCP Framework expanded and further developed to be a comprehensive set of guidelines for consent driven patient centered privacy policies. We demonstrate one possible approach in the CanCare system and Privacy Centered AC (PCAC). As more current and defunct systems are modelled, we hope to better be able to compare and contrast the relative privacy from a data owners perspective. In this way we may develop more knowable secure systems that allow individuals to manage, and understand, their privacy.
Appendix A

Scoping Review Search Queries

A.1 First Review

A.1.1 Compendex & Inspec

(((($patient) WN KY) OR (($client) WN KY)) OR (($consumer) WN KY)) and ( ((((((($health $care) WN CV)) AND (($access $control) WN CV))) ) NOT ((biometrics (access control) OR medium access control OR wireless sensor networks OR sensor nodes OR wireless telecommunication systems OR wireless local area networks (wlan) OR sensors OR body sensor networks OR quality of service OR networks (circuits) OR sensor networks OR energy utilization OR time division multiple access OR energy efficiency OR electrocardiography OR body area networks) WN CV)) NOT ((radio frequency identification (rfid) OR grid computing OR bioinformatics OR supply chains) WN CV))) AND (2004-2015 WN YR)) OR (( (($health) WN KY) AND (1896-2015 WN YR)) and ( (((($access $control) WN CV)) AND (($social $networking $online) WN CV)) AND (2004-2015 WN YR)))

A.1.2 Pubmed

A.2 Second Review

A.2.1 Compendex & Inspec

((((((patient) WN KY) OR ((client) WN KY)) OR ((consumer) WN KY))
AND (((health care WN CV) OR (health WN CV)) AND (access control WN
CV))) OR ((social networking online WN CV) AND (access control WN CV)
AND (2015-2018 WN YR)) NOT ((biometrics (access control) OR medium ac-
cess control OR wireless sensor networks OR sensor nodes OR wireless telecom-
munication systems OR wireless local area networks (wlan) OR sensors OR
body sensor networks OR quality of service OR networks (circuits) OR sensor
networks OR energy utilization OR time division multiple access OR energy
efficiency OR electrocardiography OR body area networks OR radio frequency
identification (rfid) OR grid computing OR bioinformatics OR supply chains)
WN CV))))- (artificial intelligence OR mobile telecommunication systems OR
embedded systems OR computation theory) WN CV

A.2.2 Pubmed

((“Health Records, Personal”[Mesh] OR “Consumer Health Information”[Mesh]
OR “Social Support”[Mesh]) AND (“Confidentiality”[Mesh] AND “Computer
Appendix B

Scoping Review Search Results

B.1 First Review Corpus

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>
Table B.1 – continued from previous page

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>
Table B.1 – continued from previous page

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>

Continued on next page
Table B.1 – continued from previous page

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>

Table B.1: Literature Included in First Review Corpus

---

B.2 Second Review Corpus

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. Sicuranza, A. Esposito, and M. Ciampi, “An access control model to minimize the data exchange in the information retrieval,” Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 6, pp. 741752, Dec. 2015.</td>
</tr>
</tbody>
</table>

Continued on next page
Table B.2 – continued from previous page

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Data protection issues of integrated Electronic Health Records (EHR).”</td>
</tr>
</tbody>
</table>
Table B.2 – continued from previous page

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>

Table B.2: Literature Included in Second Review Corpus
Bibliography


[38] Rafae Bhatti, Arjmand Samuel, Mohamed Eltabakh, Haseeb Amjad, and Arif Ghafoor. Engineering a policy-based system for federated healthcare databases. IEEE Transactions on Knowledge and Data Engineering, 19(9), 2007.


[42] Cátia Santos-Pereira, Luis Antunes, Ricardo Cruz-Correia, and Ana Ferreira. One way to patient empowerment.


[57] Eirini C Schiza, Georgios J Fakas, Constantinos S Pattichis, Nicolai Petkov, and Christos N Schizas. Data protection issues of integrated electronic health records


