PARTICIPATORY DESIGN RESEARCH TO INTEGRATE PRIVACY LAW REQUIREMENTS AS DESIGN REQUIREMENTS FOR PATIENT PORTAL USER INTERFACE

By

Maha Aljohani

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

at

Dalhousie University
Halifax, Nova Scotia
December 2018

Table of Contents

List of Tables

List of Figures

Abstract

The increase in privacy legislation has motivated our research on integrating privacy law requirements as design requirements. An effective privacy compliance framework requires communication between privacy professionals and IT designers. To bridge the gap between the two professions, we propose and apply mixed methods of Participatory Design (PD) techniques to collaboratively construct design ideas from multidisciplinary teams based on the legal perspective of privacy.

In focusing on enhancing the privacy of the user interface in the context of online patient portals, we aim to develop a taxonomy of a usable privacy framework derived from PD for IT designers as a one-stop-shop framework to help them show compliance with privacy legislation. We started with the requirement-gathering phase by analyzing the Nova Scotia's Personal Health Information Act (PHIA) to generate a set of privacy patterns that cover individuals' privacy rights. Next, we conducted in-depth interviews to communicate the design solutions proposed from the privacy patterns and cover gaps we discern from the initial analysis. We applied Grounded Theory to the qualitative data we collected to form a set of privacy-preserving design guidelines regarding Notification, Data Collection, Data Access, Information Disclosure, and Consents. These guidelines shape our initial privacy-preserving requirements and are used as input (tasks) to the cooperative prototyping sessions.

Our proposed cooperative prototyping sessions, as participatory design research, are divided into two studies. Three rounds of the Collaborative Analysis of Requirement and Design (CARD) was conducted to provide a high-level task analysis and used to build on our proposed privacy-preserving framework. The results from the CARD sessions were used as input to the next four Decision-Making (DM) workshops as a way to include privacy professionals and multidisciplinary teams in the early design phase. We focus on bringing diverse perspectives to construct usable and privacy-preserving collaboratively agreed-upon designs. Privacy professionals evaluated these designs during the workshops. We also apply Activity Theory as a qualitative framework to understand how multidisciplinary teams create common agreed-upon designs and share expertise as a supportive potential contribution. The final phase was combining the inputs from all the previous phases to form our proposed usable privacy-preserving framework as our main potential contribution that is Nova Scotia PHIA-compliant.

List of Abbreviations Used

AT	Activity Theory
CARD	Collaborative Analysis of Requirement and Design
DC	Data Controller
DM	Decision Making
DP	Data Processor
DS	Data Subject
EHR	Electronic Health Record
EMR	Electronic Medical Record
GT	Grounded Theory
IDI	In-Depth Interview
IT	Information Technology
PbD	Privacy-by-Design
PD	Participatory Design
PET	Privacy Enhancing Technology
PHI	Personal Health Information
PHIA	Personal Health Information Act
PHR	Personal Health Record
PIPEDA	Personal Information Protection and Electronic Documents Act
PP	Privacy Pattern
TH	Third Party

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor Dr. James Blustein for the continuous support of my Ph.D. study, for his patience, encouragement, and immense knowledge. As my supervisor, he has taught me more than I could ever give him credit for here. He has shown me, by his example, what a good scientist (and person) should be.

My sincere thanks also go to my thesis committee: Dr. Kirstie Hawkey and Prof. Carla Heggie for their insightful feedback and professional guidance, which helped me to widen my research from various perspectives. A special thank you for Dr. Kirstie Hawkey for her support and how she taught me a great deal about research.

Very special thanks to my family. I am grateful to my mother who believed in me and supported me in every step of my life and my Ph.D. Words cannot express how grateful I am to my beloved husband for encouraging me throughout this experience and supporting me through all the difficulties. I am more than grateful to my daughter for her unconditional love. Last but not least, I would like to thank my brothers and sisters for being a constant source of strength during my journey of studying overseas. I would not have been able to complete this thesis without my family's continuous support.

1 Chapter 1: Introduction

"If all information about you is readily available to anyone who wants it, you have no informational privacy. If nobody else knows anything about you, you have perfect informational privacy. All of us live between those two extremes" (David D. Friedman, 2000, p.2).

1.1 Motivation

How would IT designers comply with one privacy rule as a standard law compliance task when required to show compliance (Anton & Swire, 2014)? What would happen if the IT designer miscomprehended a privacy law at the initial step of applying a new privacy law? How would the subsequent steps be affected?

1.2 Problem Definition

The gap between privacy law language and IT privacy language is caused by a number of factors (Guarda & Zannone 2008; Compagna et al., 2009; Anton & Swire, 2014; Oliver, 2014).

First, it is difficult to fully capture the legal requirements and integrate them as design requirements due to their "technology neutral" formation and the ambiguity of the necessity of their application by designers (Compagna et al., 2009; Anton & Swire, 2014; Canada's Health Informatics Association, 2012). For example, "for lawyers, it is simple to say data minimization, [but] for engineers [designers], those two words are the beginning of a very complex process" (Anton & Swire, 2014). Another example is the word "reasonable", which appears more than 40 times in the Health Insurance Portability and Accountability Act (HIPPA) in the U.S. One designer's reaction to this term was: "How do you code 'reasonable'?" (Anton & Swire, 2014; Oliver, 2014). The rules of the acts are formulated to explain how the organization should apply these requirements in "human-run" practices, not "computer-run" procedures (Compagna et al., 2009). This point was emphasized in the Personal Health Information Act (PHIA) review recommendation report by the Information & Privacy Commissioner for Nova Scotia; Tully (2016) stated that PHIA is designed to be carried in paper-based practices, so there is a need to set clear standards when using Electronic Health Records (EHRs) in an online manner. The need to move to a digital practice is vital and is considered an emerging strategy (Moen & Bernnan, 2005). Bridging the gap between these two different disciplines is critical (Aljohani et al., 2016).

Creating communication between the two professions would produce a common language that they can share and easily apply in the digital world. It can be challenging for designers to comprehend legal language at the same time as they are managing the complexity of the systems and their development lifecycle, starting from the design requirements all the way to the evaluation of the final product (Oliver, 2014). The literature does not include having “privacy laws translators”, although translating legal requirements to practical/functional requirements has to be part of the design lifecycle.

Ramakrishna and Paschke (2014) conducted research aimed at translating legal requirements into everyday language that can be used by engineers during the design phase. However, this research is geared more to helping law experts during the design of a law from a legal perspective rather than from a technological perspective (Ramakrishna & Paschke, 2014). Przybylo et al. (2014) proposed a HIPAA-compliant group messaging (HCGM) application, which they claim, applies all the privacy principles of HIPPA; however, they do not show how the system is compliant.

A third reason for the gap is the lack of focus on the “process”. Specifically, there is presently a lack of research and documentation stating how these laws can be enforced in the digital world (Oliver, 2014). In large IT projects, some business analysts are able to translate business needs into technical rules; however, there are few, if any, legal analysts who can integrate technical requirements as design requirements as part of a team. The proposed solution is to bring these two professions together by engaging privacy professional and IT designers in the design process to provide IT designers with a one-stop-shop of methodologies and a research framework that shows them how to comply with legal requirements illustrating the steps of the research that have been tested and validated.

1.3 Research Objectives

In our context, the research area is the intersection between three different areas: privacy laws, IT service in healthcare context, and Participatory Design research as a methodology to bridge the gaps (Figure 1). The healthcare context is derived from PHIA, as it is designed to cover Personal Health Information (PHI) privacy rules. The privacy laws in healthcare are intended to address the special privacy concerns regarding the collection, use, and disclosure of personal health information. There is a need to incorporate these laws because this field is considered as an important emerging research area (Parks et al., 2011). The ultimate goal is to bridge the compliance gap between the two professions by providing designers with a privacy-preserving framework to follow in order to comply with privacy laws Canada.

To achieve the goal, we propose a mixed approach of Participatory Design research methods as a methodology to form the framework. The literature currently does not include any privacy-preserving design frameworks based on privacy law requirements in the context of healthcare applications (Essén et al., 2017). Therefore, bridging the gap between policy and practices is vital (Essén et al., 2017; Pallozzi-Ruhm & Agee, 2016).

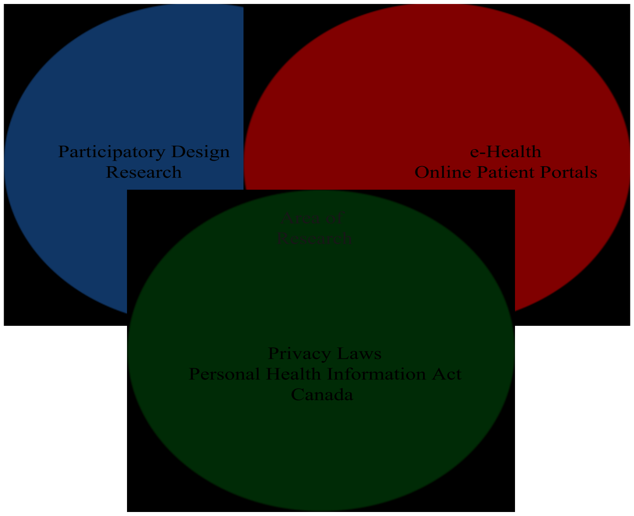


Figure 1. The research area

Another goal of this research is to explore the co-design methodologies to understand how multidisciplinary participants interact and share experience and knowledge from different perspectives, and how they create a common language through collaboratively agreed-upon designs that are usable and privacy preserving. Additionally, we would like to explore how multidisciplinary participants construct design ideas to create a common understanding and designs.

Our intention is to apply theories as analytical frameworks rather than design tools. By doing so, we explore new perspectives in HCI and PD and propose theoretical contributions. Our focus is on both Grounded Theory and Activity Theory. The proposed methodology, as explicated in Chapter 3, allows for a multidisciplinary participation of different stakeholders to act as co-designers. We support the Privacy-by-Design notion by integrating privacy requirements from the very first step of the design cycle.

At the same time, we aim to improve the flow of the design process by bringing multidisciplinary representatives into the design process as co-designers, co-evaluators, and co-owners of the design to allow for a greater level of participation and to expand the concept of end-users by including different stakeholders in the design process not only actual end-users. We intend to involve different stakeholders who are influenced by the design directly or indirectly to develop the innovative designs. These designs represent a collaborative effort, where the design process should include diverse stakeholders. Each phase of the research methodology has its own research objectives and questions, which leads to greater coverage of the research objectives outlined in this Chapter.

2 Chapter 2: Background and Related Work

2.1 Privacy

In Human-Computer Interaction (HCI) privacy is defined as the right of individuals to have control over the personal data shared online (OECD, 1980 & National Research Council, 2003). Westin (1967, p.7) defines privacy as “the claim of individuals, groups, or institutions, to determine when, how and to what extent information about them is communicated to others.” Westin’s definition of privacy overlaps with the definition of privacy from HCI research (OECD, 1980 & National Research Council, 2003). The meaning of privacy depends on the context, and it is often subjective. However, Van Rest et al. (2014, p. 59) believes “that privacy is considered a right, a freedom, a capacity, a claim and an ability”. Langheinrich (2001) has classified privacy to the following categories:

- Privacy of personal behavior (media privacy);
- Privacy of territory (territorial privacy);
- Privacy of the person (bodily privacy);
- Privacy of personal communications (interception privacy), and
- Privacy of personal data (data or information privacy).

In this thesis, we use the definition of the right to have control over the PI shared online.

2.2 Privacy-By-Design (PbD)

Privacy-By-Design guidelines propose that privacy must be integrated from the first step of the design and throughout the design lifecycle (Cavoukian, 2013). The International Privacy Commissioners and Data Protection Authorities, Ontario, Canada approved the Privacy-By-Design concept in October 2010 as an “essential component of fundamental privacy protection”. A summary of the seven Privacy-By-Design (PbD) fundamentals are summarized and shown in Table 1 (Cavoukian, 2013).

Principle	**Definition**
Proactive not Reactive; Preventative not Remedial	The main idea is to prevent personal data invasion; this requires the consideration of privacy in the early design stages.

Principle	**Definition**
Privacy as the Default Setting	Automatically protect personal information. The settings that ensure privacy should not be changed unless the user wants to share their data.
Privacy Embedded into Design	Privacy should not be an add-on to systems as it used to be. It should be embedded throughout the system lifecycle at every stage.
Full Functionality: Positive-Sum, not Zero-Sum	Privacy goals and system requirements should be considered as a *positive-sum* not in a state of trade-offs between other system aspects such as security. *Positive-sum* means, "embedding privacy from the outset, other business requirements, such as security and risk management, can be met without compromise". It means that if privacy is planned from the first stage of the design cycle, it is not going to contradict with other requirements and can provide privacy by default.
End-to-End Security — Full Lifecycle Protection	Privacy should be considered before even collecting the system data and continues to be considered until the release of the system to form end-to-end cycle.
Visibility and Transparency — Keep it Open	All stakeholders and third parties who are involved in any aspect of the system should operate according to "promises" and rules should remain clear and transparent.
Respect for User Privacy — Keep it User-Centric	Designers should keep users' interests at the top of their priority list by providing privacy by default settings, notices, and more usable options.

Table 1. Privacy-By-Design (PbD) Fundamentals, (Cavoukian, 2013; privacybydesign.ca)

Besides the Privacy-by-Design concept, there are a variety of privacy design guidelines to support designers in integrating privacy in the design lifecycle (Compagna et al., 2009). Examples include Privacy Impact Assessment (PIA) (Clarke, 2009), ISO 29100 Privacy Framework Principles, Process-Oriented Strategies and Privacy Enhancing Tools (PETs) (Hoepman, 2014). However, these guidelines do not show how they can be applied, and they cover the institutional and developer perspective rather than the user perspective (Cavoukian, 2014 & Gürses et al., 2011 & Van Rest et al., 2012).

2.3 Hard Privacy vs. Soft Privacy

Deneize (2007) distinguishes between hard and soft privacy. The goal of data protection in hard privacy is to provide as limited information as possible (as a Data subject) which reduces the need to rely on Data Controllers to preserve the information's privacy. The goal refers as well to data minimization and protection from the taxonomic terms that are proposed by Solove (2006) including: surveillance, interrogation, aggregation, and identification. The privacy threat in this case is the Data Controller who might not be trustworthy (Deneize, 2007).

On the contrary, soft privacy is derived from the idea that the Data Subject has limited or no control over the personal information; in which case, the responsibility of protecting the data is shifted to data controllers who implement access control mechanisms and processing the information according to a purpose and consent. The privacy threat comes from third parties and insider errors (Deng, 2010).

In this thesis, we consider a mix between hard and soft privacy. The part of hard privacy is that DS can limit the access to the PI, which limits the amount of PI shared. The part of soft privacy is about providing design guidelines for applying privacy by default, which include our proposed privacy patterns. We focus on informing DS about the PI that is being processed with a clear purpose and consent to cover a part of the soft privacy with a level of control is shifted to the DS. We believe that it is a joint responsibility between DS and DC. Data Controller should implement techniques that help Data Subjects to have control over the PI. We believe if only DSs have control over the privacy, DSs will have no control over their PI. To comply with the definition of privacy that we are following in this research, we need to ensure that DSs have the right to have a level of control over their PI. We focus on the DS because we only cover individual rights from Personal Health Information Act (PHIA), and the organizations' responsibilities are out of the scope.

2.4 Usable Privacy

Usable privacy is mostly connected to the limiting access to personal information and control over the information shared online as suggested by Lorrie Cranor who is a leading researcher in usable privacy projects.

An example of usable privacy is the work that has been conducted by Balebako & Cranor (2014). It mainly focuses on educating developers on how to understand privacy and embedded it into the design of applications. The research outlines the issues that contribute to not integrating privacy into the App designs including developers find privacy policies hard to read, and privacy is not end-users primary tasks (Balebako & Cranor, 2014).

Schaub et al. (2015) and Cranor (2012) addressed the need for design guidelines that developers and designers can adopt that can [positively] impact the effectiveness of privacy notices, which are the main focus of their research. They proposed a taxonomy of design guidelines related to Timing (set-up, just in time, context-dependent, periodic, persistent, and on-demand) of sending notifications to end-users; Modality (visual, auditory, haptic, and machine-readable), and control (blocking, non-blocking and decoupled). The proposed guidelines help designers identify notice and choice requirements (Schaub et al.,2015).

The research of Acquisti et al. (2017) focuses on suggesting nudges to improve end users' security and privacy choices. These nudges or “interventions” aim to increase individuals and organizations awareness to help them make informed decisions based on exploring individuals’ behaviors. This paper outlines a defined path for future research directions that can be taken by researchers to fill the research gaps and design usable privacy and security systems.

Assal & Chiasson (2018) interviewed developers to explore how they carry out practices to ensure security compliance. The participants showed that best practices from their literature review are often avoided because they increase the difficulties and challenges that developers face during the design and code of security systems.

2.5 Personal Health Information Act in Nova Scotia

“The purpose of [Nova Scotia's] PHIA is to provide a framework that strikes a balance between the protection of personal health information and the collection, use and, disclosure of personal health information within (or by) the healthcare sector to deliver and improve health care services. The goal of the Act is to have comprehensive, consistent, and clear rules to help personal health information flow efficiently and effectively in the health sector” (NSPHIA, 2013). Figure 2 shows the provincial Personal Health Information Acts across Canada (Iwaskow & Russell, 2015).

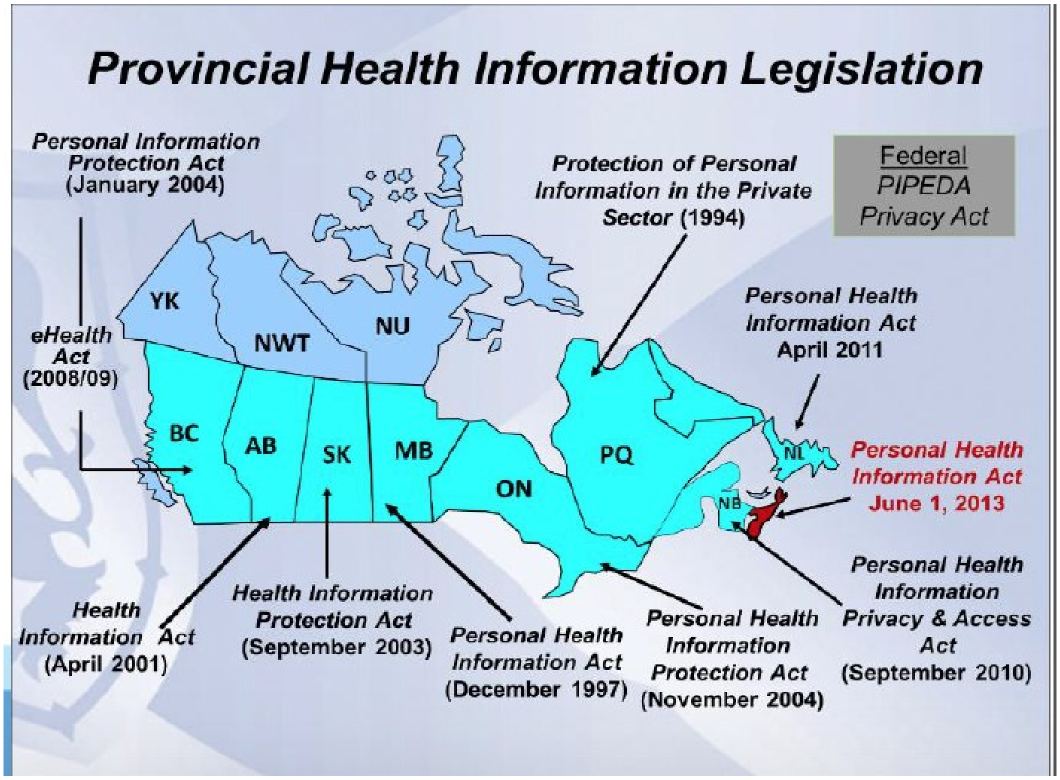

Provincial Health Information Legislation
Personal Information Protection Act (January 2004)
eHealth Act (2008/09)
Protection of Personal Information in the Private Sector (1994)
Federal
PIPEDA
Privacy Act
Personal Health Information Act April 2011
Personal Health Information Act June 1, 2013
YK
NWT
NU
BC
AB
SK
MB
ON
PQ
NL
NB
Health Information Act (April 2001)
Health Information Protection Act (September 2003)
Personal Health Information Act (December 1997)
Personal Health Information Protection Act (November 2004)
Personal Health Information Privacy & Access Act (September 2010)

Figure 2. Provincial health information legislation (Iwaskow & Russell, 2015)

2.6 PHI, EMR, EHR, and PHR

Personal Health Information (PHI) can be considered any information that identifies an individual. This information can be related to one or more of the following aspects regarding a specific individual: physical or mental health; the application, assessment, eligibility and provision of healthcare, including the identification of a person as a provider of healthcare; payments or eligibility for healthcare; registration information, including health-card number; and substitute decision-maker (Health and Wellness, 2016).

References to EMRs, EHRs and PHRs are often treated as synonyms because of how subtle the difference can appear to outsiders not intimately familiar with the different types of users, data, and technologies (Hodge & Giokas, 2011). However, they do differ. Hodge and Giokas (2011) identify these differences as follows:

- Electronic Medical Record (EMR) is often described as a provider-centric or health organization-centric health record of a person.
- Electronic Health Record (EHR) is often described as a person-centric health record, which can be used by many approved health care providers or health care organizations.
- Personal Health Record (PHR) a patient-centric health record.

Overlapping definitions are discussed by Heart et al. (2017). According to them, EMRs and EHRs are used mainly by physicians to improve the quality of care. EMR is considered an "internal organizational system" while EHR is an "intra-organizational system" where healthcare providers can exchange PHI. PHRs are managed by patients and can be connected and integrated into EMRs and EHRs. By learning the differences, designers and patients can know what to expect regarding how PHI is managed.

In our research, we outline the differences between the four concepts of EMR, HER, PHR and PHI because understanding what constitutes an EMR helps to better understand the current practices, as shown in Figure 3 in the case context in Chapter 3. As well, because the literature review lacks a clear definition of EMR, this could lead to confusion regarding the flow of PHI in healthcare systems (Hodge & Giokas, 2011).

2.7 E-Health

Privacy in healthcare has received increased interest because patients are now more active in the decision-making process of their health status (Swan, 2009). Technology innovations in eHealth allow patients to access their Personal Health Information stored online (Anderson & Agarwal, 2011). Privacy in Healthcare is a multidimensional construct including Informational, Physical and Psychological Privacy (Serenko & Fan, 2013).

Our focus is on Informational Privacy which represents patients' control over their personal information regarding the collection, storage, sharing and use. The concept of Informational Privacy and the definition of privacy in HCI along with the patients' privacy rights supported by PHIA are overlapping and share fundamental aspects of Personal Health Information privacy.

Information obtained from patients by the healthcare providers, through whatever means, is sensitive and patients would expect that healthcare provider to ensure that their data remains private (Serenko & Fan, 2013).

Appari & Johnson (2010) conducted a systematic review to investigate the current state of privacy and security in healthcare in the US. They state that threats to patient information can be classified into the two broad areas including organizational and systematic risks. They covered some technological solutions to protect patient health information from the network perspective but not the patient perspective.

Another work is conducted by Breaux & Antón, (2008) focused on proposing a methodology to help designers analyze the actual texts of regulations to outline the functional software requirements. The methodology focuses on ways to extract access rights and obligations to ensure legal compliance (Breaux & Antón, 2008). Our research is different because we focus on the individual-UI designs and individuals' rights, not the functional requirements.

2.7.1 Online Patient Portals

Online patient portals are information technologies used in healthcare to enhance the communication between patient and healthcare providers as well as to increase the participation of the patient in their own healthcare (Sun et al., 2013). Online patient portals are considered one type of PHRs. The authorized custodian who is responsible for securing and controlling the personal health information in the online patient portal is the health facility from where a patient is admitted (COACH, 2012).

Researchers are interested in the online patient portals' level of adoption by end-users (Archer et al., 2011); the main tasks patients can perform to enhance online communication between patients and healthcare providers (Sun et al., 2013); and barriers patients face during the communication (Mories, 2001).

However, the research on design guidelines is limited. Pai and Haung (2011) proposed Technology Acceptance Model that can be applied to the introduction of new healthcare technologies that increases patients' acceptance and adoption. Wilson and Lankton (2004) developed a model to predict the adoption level of online patients' portals depending on actors including, prior experience with offline systems and chronic conditions that need ongoing checking.

Miller et al. (2016) developed a set of design guidelines that could benefit designers of online patient portals. However, they did not cover the privacy of patient PHI and privacy-preserving design consideration. The Canada Health Information Association (COACH, 2012) proposed design guidelines to protect PHI; however, they focus on usability aspect, defining some functionality by investigating portal models and types, operational aspects in a broad manner.

We believe that our research methodology will bridge the gaps in the literature by focusing on the privacy-preserving designs guidelines that are prototyped by multiple stakeholders to fit the healthcare context and evaluated to ensure acceptance. We covered the online patient portals research because we aim to work on the user interface of the patient portals to deliver a level of control over their PHI.

2.8 Participatory Design

In this section, we define participation as the main aspect in participatory design, PD in Computer Science, the history of PD, PD research methodologies, tools and techniques, and PD in eHealth.

2.8.1 What is Participation?

The concept of participation is key in a variety of domains that require engagements such as community development, healthcare, architecture and agricultural development (Harder et al., 2013). Participation from an IT perspective is the notion of end-user engagement through the design life cycle (Pilemalm & Timpka, 2008). “Participation [is how] stakeholders – especially users, developers and planners – cooperatively make or adjust systems, technologies and artefacts in ways which fit more appropriately to the needs of those who are going to use them.” (Simonsen & Robertson, 2012. p. 41).

Stakeholders, other than designers and researchers, will have different levels at which their contributions could affect the final decision of technology development (Gutiérrez, 2008). Stakeholder participation can entail giving them a voice to strategically introduce them into decision-making and implementation process. This form of participation is referred to as representative participation.

In our context, the application of PD methods in healthcare is motivated from the technological perspective. Expanding the borders of end-users to include all stakeholders, who affect the design, is key to the technology development. The involvement of different stakeholders and domain experts can lead to effective and usable systems (Pilemalm & Timpka, 2008).

2.8.2 What is Participatory Design

Participatory design is a process that involves different stakeholders working together to design a solution. Participatory Design (PD) “can lead to hybrid experiences – that is, practices that take place neither in the users’ domain, nor in the technology developers’ domain, but in an ‘in-between’ region that shares attributes of both spaces” (Muller & Druin, 2003, p. 2).

The field of PD is extremely diverse including fields of user-centered design, graphic design, software engineering, architecture, public policy, psychology, anthropology, sociology, labor studies, communication studies, and political science (Gregory, 2003). In Computer Science, Participatory Design (PD) is a set of theories, practices, and studies related to end-users as full participants in activities leading to software and hardware computer products and computer-based activities (Greenbaum and Kyng, 1991; Muller and Druin, 2003; Schuler and Namioka, 1993). Suchman (2002) described the experience of PD in research as "working for the presence of multiple voices not only in knowledge but in the production of technologies as knowledge sources objectified in a particular way." Bodker and Buur (2002) noted there is a need to support the "many-voiced nature of design." PD leads to the invention of very sophisticated and unique solutions that could not have been met by a sole design team. The shared decision-making approach aims at ensuring that the usability of the solution is efficient and effective in meeting the end-user demands.

2.8.3 The History of Participatory Design

A historical summary of participatory design dates the approach back to the early 1970s when two Norwegian research programs were in the bid to empower workers who worked in technological industries or those whose duties could incorporate technology (Ehn, 2016). The first generation of PD methods in IT systems mainly focused on "collective designs" or collective resources research where engaging employees or workers in the production of technologies to improve their production and performance (Ehn, 2016). The second generation of PD was the result of shifting participation from the context of employment and workers into social and commercial settings (Pilemalm & Timpka, 2008; Ehn, 2016). The socio-technical systems design program focused on worker empowerment by British Researchers. It has been argued that the participation of end-users in the second generation resulted in more usable systems (Tollmar, 2001; Oostveen & Besselar, 2004; Pilemalm & Timpka, 2008; Ehn, 2016). However, PD was implemented in small-scale and stand-alone IT services. The future third generation of PD is to expand in the domains and areas that PD can be applied to cover health care practices and health informatics to make user participation applicable to large-scale information systems and health information management services (Pilemalm & Timpka, 2008).

2.8.4 Participatory Design Research Methodologies, Tools and Techniques

Participatory Design is a collection of participatory methods, techniques, and tools that facilitate users participation (Spinuzzi, 2005). The tools, methodologies, and techniques differ depending on the context for which the stakeholders are operating as well as the way they are put together (Sanders, Brandt & Binder, 2010). PD is as an umbrella that covers various research methods including interviews, ethnographic observations, focus groups, workshops and cooperative prototyping techniques (Spinuzzi, 2005; Krishnaswamy, 2012; Krishnaswamy, 2004; Bergold & Thomas, 2012; Muller & Druin, 2010; Brandt, 2012). In every example of PD research, there are three primary stages, initial exploration, discovery processes, and prototyping (Spinuzzi, 2004). We have adopted the primary stages of PD research to map the methods from the literature review as explained in the following sections:

2.8.4.1 Initial exploration stage

In the initial phase, it mainly focuses on the understanding and exploring the design problem. Designers usually meet with end-users to collect data about how tasks are performed. The exploration should involve not only end-users should be taken into account but also procedures, routines and other aspects of performing current practices (Spinuzzi, 2004). Examples of methods that can be used in this stage include ethnographic observations and interviews, which focus mainly on the design problem and its description (Wall and Mosher 1994). We can map the privacy patterns and the in-depth interview study that we conducted to this stage of PD research.

2.8.4.2 Discovery processes stage

In the discovery process phase, designers and users apply techniques to clarify the software and end-users goals, values and desired outcomes (Spinuzzi, 2004). The most interaction between the designers and end-user occurs at this stage. As it is named, it is a discovery process where the work is cooperatively discovered instead of only described. Examples of methods used in this stage include role-playing games (Iacucci et al., 2000), future workshops (Bodker et al., 1993, p.164; Bertelsen 1996), storyboarding (Madsen & Aiken 1993), workflow models (Beyer & Holtzblatt 1998). We can map the initial session in our research to this stage.

2.8.4.3 Prototyping stage

At the stage of the prototyping, designers and end-users iterate and shape the designs. The prototyping can have different forms ranging from low fidelity to working prototype. There are a variety of techniques that can be applied in this stage including mockups (Ehn 1989; Ehn & Kyng 1991, paper prototyping (Novick, 2000), cooperative prototyping (Bødker & Grønbæk, 1991) and PICTIVE (Muller 1991b, 1993). We can map the cooperative prototyping sessions that we plan to conduct to the discovery process phase.

2.8.5 Participatory Design in eHealth

Participatory Design in healthcare context is emerging where end-users take part in the development process of the IT service (Rothmann et al., 2016; Pilemalm & Timpka, 2008). Healthcare systems are complex due to the different types of entities involved and professions leading to various types of challenges (Pilemalm & Timpka, 2008; Kripalani et al., 2007). The participation (involvement) of all stakeholders in the design process is essential to overcome these challenges and lead to technologically effective and usable systems (Pilemalm & Timpka, 2008; Hibbard & Greene, 2013; and Dykes et al., 2014). It is considered as productive research approach shifting the focus to co-designing (Danbjørg, 2016; Holm et al., 2016; Davidson & Jensen, 2013).

In a healthcare setting, the interaction (co-designing) is not exclusively applied to the medical staff but also including anyone who would influence the design including patients, and health professionals (Grönvall & Kyng, 2013). PD is introduced in new areas for healthcare services that are out of the workplace such as home technologies to help older patients participate in their health care (Grönvall & Kyng, 2013). Another example is considering elderly as co-designers which resulted in developing creative design ideas (Davidson & Jensen, 2013). Experience-based Co-design (EBCD) is a PD approach focused on the involvement of healthcare staff and patients to improve quality of care and was proposed by (Donetto et al., 2015). The challenges resulted from applying the EBCD approach illustrates a need for a cross-discipline research effort to bridge the gaps and draw a complete picture of practices evolved in the design, their design principles and goals (Donetto et al., 2015).

3 Chapter 3: Participatory Design Research Methodology

In this chapter, we apply Participatory Design (PD) research to the development of an effective privacy compliance framework in the context of healthcare applications provided to IT designers. We aim to bridge the gap between privacy law designers and privacy IT designers by expanding the concept of end-user participation. We propose and apply mixed methods of Participatory Design (PD) techniques to collaboratively construct design ideas from multidisciplinary teams based on a legal perspective of privacy, and to facilitate the participation of different stakeholders during the design lifecycle.

3.1 PD as a Third Space

Participatory Design is considered a third space in HCI between technology development and end-users (Muller and Druin, 2002). Each space has its own knowledge and practices, as noted by Suchman (2002), but the movement between these two spaces is considered challenging (Olsson, 2004; Reymen et al., 2005; Yamauchi, 2009). Having a hybrid space as a third space would help shed light on developing new practices and knowledge. We aim to facilitate two-way interactions through our proposed methodology, and believe this proposed hybridity will also lead to greater novelty and creativity.

3.2 Justification for the Methodology

We applied mixed methods of PD to fulfill our research purposes, for several reasons.

First, PD provides a richer contextualized communication medium. Participatory Design methods aim at increasing technological democracy via early engagement of different stakeholders who would have a "say" in the design process (Bjögvinsson et al., 2010). Their input would thus have significant implications on the external and internal designs of IT systems. Our setting supports the concepts of co-design and co-evaluation by all stakeholders who are influenced directly or indirectly by the technology (Binder 2007; Björgvinsson et al., 2010). Bygholm and Kanstrup (2017) elaborated on the need for co-design workshops in real-life contexts to develop Health Information Technology, and Buur and Mathews (2008) conducted several studies to explore PD methods. However, while technology garners most of these researchers' focus, the system users and context receive far less attention.

So, to cover both the people and the context, we base our PD research on the analysis of current practices in the province of Nova Scotia because we want to create a link between the context and the technology's analysis and design by working on a real case. We provide analysis of PHIA from a technological point of view and try to understand how practices are performed regarding protecting patients' PHI. By using it as a real case, we believe other researchers in Nova Scotia will better understand how the approach is applied, while inspiring researchers from other provinces to apply and compare our findings with theirs.

A second reason why we used mixed methods of PD is that this method provides more productive communication and enhanced sharing through the combination of diverse perspectives, leading to stronger engagement (Krishnaswamy, 2004; Muller & Druin, 2002; Kanstrup et al., 2017b). Applying PD in healthcare technology is evolving, and the complexity of the context requires the hyper exchange of knowledge and expertise (Kanstrup et al., 2017a). We need such an exchange, especially in healthcare where the context is so complex and fluid (Kanstrup et al., 2017a).

Third, using mixed methods of PD helps to build bridges between software professionals and other stakeholders. Recognizing different perspectives and reducing conflicts when sharing knowledge from multidisciplinary views is a claimed benefit, according to Krishnaswamy (2004). The PD design strategy covers the strengths possessed by the team and exploits their skills and competencies (Bergold & Thomas, 2012, p. 201). Research performed by Bjögvinsson and Hillgren (2012) proved that the 'open dialogue' nature of the program fosters the understanding that there are multiple suggestions and positions in relation to the problem at hand. As a result, the stakeholders develop a more nuanced perception of the issues and thus enhance their openness to explore new possibilities towards solutions.

3.3 Our Case Context

The flow of information in eHealth is highly complex. As a first step towards unraveling the complexity, we define the context to which we apply the methodology to the research problem and address the research questions. A conceptual diagram of the context is shown in Figure 3. The flow of PHI is derived from the analysis we have performed on currently available Nova Scotia EMRs, online portal (MyHealthNS[1]), and the context at which our contribution is aimed.

[1] https://www.myhealthns.ca

In addition, we want to cover the research questions according to the following context, as shown in Figure 3. Individuals can access their PHI through an online patient portal that is connected to their EMR. The EMR is connected through portals to other sources of PHI, such as lab results, diagnoses, medical records, and imaging. Office administrators and family physicians can also access, edit, and make changes to the patients' EMRs.

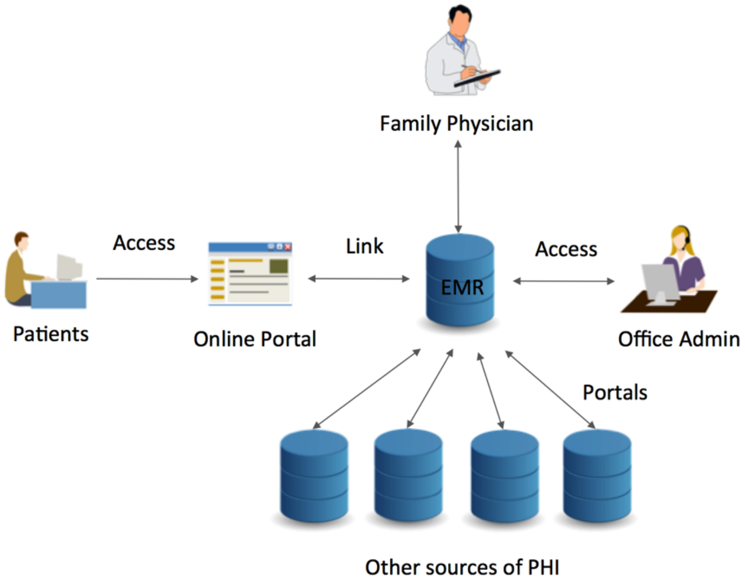


Figure 3. The case context

3.4 Methodology Model

We are motivated to focus on applying methods of Participatory Design research due the need for interdisciplinary knowledge exchanges from different stakeholders. The proposed PD research approach is divided into five phases, as shown in Figure 4 and as discussed in the following sections.

3.4.1 Phase 1: PHIA Analysis

In this phase, we applied an extensive analysis and built our background of patients' rights under PHIA. We designed a privacy pattern that addresses each privacy right in order to cover legal aspects. The template we followed in forming the proposed privacy patterns was derived from the Pattern-Oriented Software Architecture (POSA2) outline as a simplified version. POSA2 was developed by Buschmann et al. (1996; 2007) and applied by Romanosky et al. (2006) when creating privacy patterns. We discussed each pattern by explaining the context, problem, proposed solution, consequences, related patterns, and use cases. We added consequences and security assumptions to the POSA2 template. Then, we proposed the privacy design patterns in the context of healthcare systems. These patterns are designed to support the Privacy-by-Design concept through the software lifecycle, focusing on the early design phase. As a departure point, we used the Personal Health Information Act in Nova Scotia to derive the following four proposed privacy patterns that are named according to individuals' rights:

1- Access Pattern
2- Correction Pattern
3- Limit Disclosure Pattern
4- Notification Pattern

The four patterns provide a guide to designers and developers in providing solutions for privacy problems while designing privacy-preserving systems in healthcare from individuals' perspectives. To validate the proposed patterns, they were mapped to the ISO 29100 Privacy Framework Principles and Process-Oriented Strategies. The outcome of the mapping process showed that most of the ISO 29100 principles are covered, with suggestions and recommendations being provided for the uncovered principles. All four Process-Oriented Strategies were mapped and covered by the proposed patterns. A full description of the proposed patterns is given in Chapter 4.

3.4.2 Phase 2: Requirements Gathering- In-depth Interview Study

In this phase of the project, we aimed at collecting qualitative data from different stakeholders to draw a complete picture of current practices, challenges, knowledge, experience, perceptions and future recommendations in relation to managing Electronic Health Records through online portals as the first research phase. The primary objective of the interview study is to form privacy-preserving design guidelines based on privacy laws that cover PHIA rules from the legal perspective as well as privacy law and current practices in managing Personal Health Information from information technological and managerial perspectives. A supporting goal is to take the first step toward bridging the gap between IT designers and Law representatives by collecting qualitative data from different stakeholders to draw a complete picture of current practices, challenges, knowledge, experience, perception and future recommendation with regard to managing PHI in general and through online portals. For better understanding and exploration, we need to cover technological, managerial and legal perspectives.

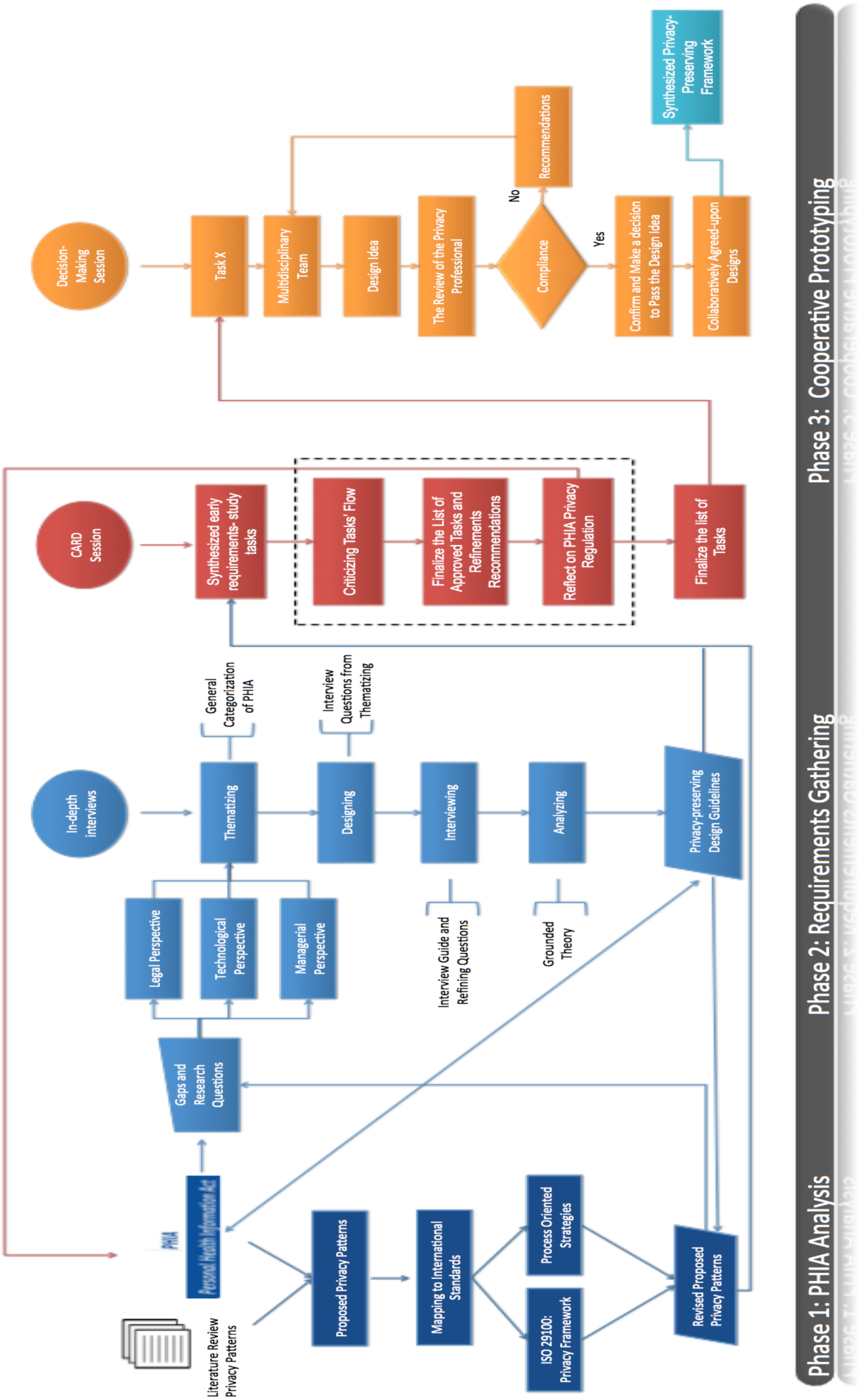

Phase 1: PHIA Analysis
Phase 2: Requirements Gathering
Phase 3: Cooperative Prototyping
Literature Review
Privacy Patterns
PHIA
Personal Health Information Act
Proposed Privacy Patterns
Mapping to International Standards
ISO 29100: Privacy Framework
Process Oriented Strategies
Revised Proposed Privacy Patterns
Gaps and Research Questions
Legal Perspective
Technological Perspective
Managerial Perspective
In-depth interviews
Thematizing
General Categorization of PHIA
Designing
Interview Questions from Thematizing
Interviewing
Interview Guide and Refining Questions
Analyzing
Grounded Theory
Privacy-preserving Design Guidelines
CARD Session
Synthesized early requirements- study tasks
Criticizing Tasks' Flow
Finalize the List of Approved Tasks and Refinements Recommendations
Reflect on PHIA Privacy Regulation
Finalize the list of Tasks
Decision-Making Session
Task X
Multidisciplinary Team
Design Idea
The Review of the Privacy Professional
Compliance
No
Recommendations
Yes
Confirm and Make a decision to Pass the Design Idea
Collaboratively Agreed-upon Designs
Synthesized Privacy-Preserving Framework

Figure 4. Participatory Design research methodology

The process of designing the study by conducting in-depth interviews underwent many stages, including Thematizing, Designing, Interviewing, Analyzing, and Proposing privacy-preserving design guidelines. We applied Grounded Theory as an analytical approach to form the privacy-preserving guidelines. We derived themes related to Personal Health Information access, breach conditions, Electronic Medical Records, and Privacy Legislation Compliance. Based on the results, we propose several privacy-preserving design guidelines to help IT privacy designers show compliance with privacy legislation in the design process of online patient portals in Canada. The output of the study, combined with the privacy patterns proposed in Phase 1 is used to form the tasks of the following stage, which is a Participatory Design workshop in the form of Cooperative Prototyping. A full description of the study objectives, methodology, analysis process and results is presented in Chapter 5.

3.4.3 Phase 3: Cooperative Prototyping Sessions

Participatory prototyping is an iterative process in which stakeholders integrate both the analysis phase as well as the phase covering the actual development of the desired product. The primary advantage of participatory prototyping is that it creates an environment where gaining feedback from all relevant stakeholders is possible (Waart et al., 2015).

We want to apply cooperative prototyping approaches as PD research to gain feedback from different stakeholders who are considered PHIA users in the e-Health context. A supporting goal is to facilitate a higher degree of multidisciplinary collaboration on design issues, which will lead to creative design solutions. As well, we aim to provide a mutual learning process between all stakeholders who are involved in the design process. The research methodology is designed in a way to focus on how we integrate privacy law requirements as design requirements; how all-multidisciplinary participants interact, criticize, evaluate and create common agreed-upon designs; and how they share their expertise and experience.

In addition to collecting data during the sessions, we plan Activity Theory as a qualitative analytical framework. Activity Theory is “a philosophical and cross-disciplinary framework for studying different forms of human practices as development processes, [with] both individual and social levels interlinked at the same time” (Bardram, 1997). We focus on exploring how to apply AT in PD research as an analytical method. It is applied to understand how multidisciplinary participants construct design ideas in the context of privacy-preserving designs for eHealth applications.

There are three cooperative prototyping sessions: an initial session that applies the CARD method (Tudor et al., 1993; Muller et al., 1997), and two productive sessions where we propose and apply our Decision-Making PD workshop.

A full description of the study research questions, as well as the study process in each session is presented in detail in Chapter 6.

3.4.3.1 CARD Sessions

The reason for applying Collaborative Analysis Requirement Design (CARD) is to analyze, criticize and redesign the task flows, which prepare the task scenarios for the subsequent sessions. We recruited only IT designers from different backgrounds for the CARD sessions. The output is a high-level task analysis of our initial privacy-preserving requirements.

3.4.3.2 Decision Making Workshops

The objectives of the DM workshops include: exploring the scenarios based on tasks and focusing on the flow of information and how users interact with each step; communicating privacy-preserving solutions in the form of usable designs; and ensuring active participation in the design process of all participants in the sessions to gain different feedback points from different backgrounds.

Our intention is to focus on having a privacy professional in the workshop in the early design phase. The feedback at this stage of design add to the validity of the designs to ensure compliance. We plan to have at least two rounds of productive sessions. Participants of the DM workshops are multidisciplinary teams of IT Designers, Patients, and Privacy Professionals.

The output of the workshops, combined with the sequential contributions from previous phases, is used to build our privacy-preserving framework in the context of an online patient portal.

Overview of research design phases, methods and outcomes in shown in the following Table 2:

Phase	Type of Study	Study Sample	Methods	Data Collection methods	Data Analysis Tools
Phase 1: PHIA analysis and privacy patterns	Literature review study	Seventy privacy patterns were reviewed and four are proposed.	Privacy Patterns Technique	• Systematic review of 70 patterns from the literature review • NSPHIA toolkit and NSPHIA for public • MyHealthNS report	• ATLAS.ti • Mapping to ISO 29100 privacy framework and Process Oriented Standards
Outcome of phase 1: we propose privacy design patterns in the context of healthcare systems including: Access Pattern, Correction Pattern, Limit Disclosure Pattern and Notification Pattern to cover PHIA individual rights.					
Phase 2: Requirement gathering and current practice	In-depth Interview Study	8 participants	Qualitative	• Demographic questionnaires • Semi-structured interviews	• Grounded Theory • Excel (demographic data) • ATLAS.ti
Outcome of phase 2: It includes the proposed privacy-preserving design guidelines that cover the technological, legal and administration perspectives based on the current practices. It involves suggestions to PHIA rules and ways to expand the study.					
Phase 3 Part 1: Cooperative Prototyping-Initial Sessions	Collaborative Analysis of Requirement and Design	12 Participants Who are all IT Designers	Qualitative	• Tasks • Pre- and Post Study questionnaires • Audio and Video tapes for design surface • Observation notes Design Sketches	• Content analysis • Activity Theory • Excel (demographic data) • ATLAS.ti
Outcome of phase 3 Part 1: High-level task analyses and a list of design tasks that are based on the design guidelines from the previous phase. The tasks are mapped to the ISO 29100 privacy principles, linked to the privacy patterns and classified based on categories including access, notifications, consents, and limiting data disclosure tasks.					
Phase 3.2: Cooperative Prototyping-Productive Sessions	Decision Making Workshop	18 total: 2 Privacy Professionals 8 IT Designers 8 General Public (Patients)	Qualitative	• Tasks • Pre- and Post Study questionnaires • Audio and Video tapes for design surface • Observation notes Design Sketches	• Content analysis • Activity Theory • Excel (demographic data) • ATLAS.ti
Outcome of phase 3 Part 2: This phase covered main categories were discussed, collaboratively agreed-upon designs, and our proposed privacy-preserving framework.					

Table 2. Overview of research design phases, methodology and outcomes

4 Chapter 4: Phase One: Privacy Patterns

4.1 Introduction

In this Chapter, we propose privacy design patterns in the context of healthcare systems. These patterns are designed to support the Privacy-by-Design concept through the software lifecycle, focusing on the early design phase and mitigating privacy risks. As a departure point, we used Personal Health Information Act (PHIA) in Nova Scotia to derive the following four proposed privacy patterns: Access Pattern, Correction Pattern, Limit access pattern, Notification Pattern.

The patterns provide a guide to early privacy-preserving requirement gathering process and as an input to the following research phase, the in-depth interview study.

4.2 Research Objectives

Laws and legislation alone do not prevent individuals from giving personal information nor prevent anyone from gaining access to someone else's personal information without permission. We use the privacy patterns as a method to translate privacy requirements from legal perspective into design perspective (Chung et al., 2004). Privacy patterns are privacy design guidelines that can be used early in design lifecycles. Privacy Patterns supports the concept of Privacy-by-Design (PbD), which is essential because it suggests that privacy must be integrated from the first design steps, and maintains such care throughout the design lifecycle (Cavoukian, 2013). Therefore, design privacy patterns are proposed to protect personal information by design and default.

Proposing privacy patterns is motivated by the need to bridge the compliance gap between privacy laws and their application. At the same time, another motivation is to maintain levels of privacy as NSPHIA is designed to be applied through hard copies, which are transferred into digital artifacts (Tully, 2016).

The overall objective of the research is to provide Information Technology (IT) and UI designers and developers with privacy design guidelines and a method that cover privacy rights according to Personal Health Information Act (NSPHIA) and integrate privacy rights as privacy requirements. This will help designers to answer the question: How can we incorporate privacy laws and legislation as privacy requirements into privacy design? The proposed patterns are designed from an HCI and user interface perspective.

Another goal is to validate whether the proposed Privacy Patterns can be mapped to international standards-based methodologies (e.g., ISO 29100) to answer the questions: What privacy principles are guaranteed if the system design followed the proposed patterns? Our proposed patterns are considered as the first phase of the research approach of the Ph.D. thesis.

4.3 Related Work

Privacy patterns are designed guidelines that can be used in similar contexts (Chung et al., 2004; Dingledine et al., 2004). Privacy patterns are structured to state a problem and propose solutions followed by known uses and related or similar patterns. We have studied 13 out of 70 privacy patterns as shown in Figure 5. Examples of literature review of patterns are described in the sections that follow:

4.3.1 Informed Consent

Informed Consent for Web-Based Transaction Pattern was developed by Romanosky et al. (2006). When collecting personal information, websites often employ so-called cookies. Users are concerned that their personal information would be collected and used without their consent or not want to share their personal information. The problem rests on how designers can have a balance between the reasons for using the PHI and the users' concerns about how their PHI is used. To solve the problem, the web designer should provide the user with the following elements: disclosure, agreement, comprehension, voluntariness, competence, and minimal distraction. The patterns have been used in many well-known websites, such as Yahoo, Google and ehealthinsurance.com during the filling of the registration form. Similar patterns include informed consent (Fischer-Hübnner et al., 2010; Compagna et al., 2009), need-to-know (Compagna et al., 2009) and obtaining explicit consent pattern by Porekar et al. (2008).

4.3.2 Access Data

Porekar et al. (2008) designed the Access Control to Sensitive Data Based on Purpose to solve the problem of allowing individuals to be informed of the purpose of collecting information. The user should have the ability to decide which aspect or piece of information a third party should be allowed to have access. The pattern applies the Need-to-know mechanism to limit the amount of sensitive information transmitted to third parties. The pattern provides access to only what the user gives permission to be accessed. The Platform for Privacy Preferences (P3P) is the well-known use of the pattern (W3C, 2002).

4.3.3 Feedback

Ambient notice solves the problem when the users' location information is used as a repeated model dialog with or without the users' permission (Privacy Patterns, 2015). How can users get a notice about every time a service is pulling location information? An ambient notice that appears instantly when location information is retrieved.is considered being the solution. The notice should provide an opportunity for interaction regarding permissions. Known uses of the pattern are the location-based service icons used in Mac OS/X where is it shown as a compass arrow that appears in the taskbar every time a software program is used identify the user's location. Other patterns include outsourcing and non-repudiation by (Compagna et al., 2009), data abstraction by (Bier & Krempel, 2012) privacy dashboards, private link by (Privacy Patterns, 2015), and instant user interface for information about personal identification information by (Bier & Krempel, 2012).

The results of the synthesized literature review include the following privacy patterns and the relationship between them as shown in Figure 5.

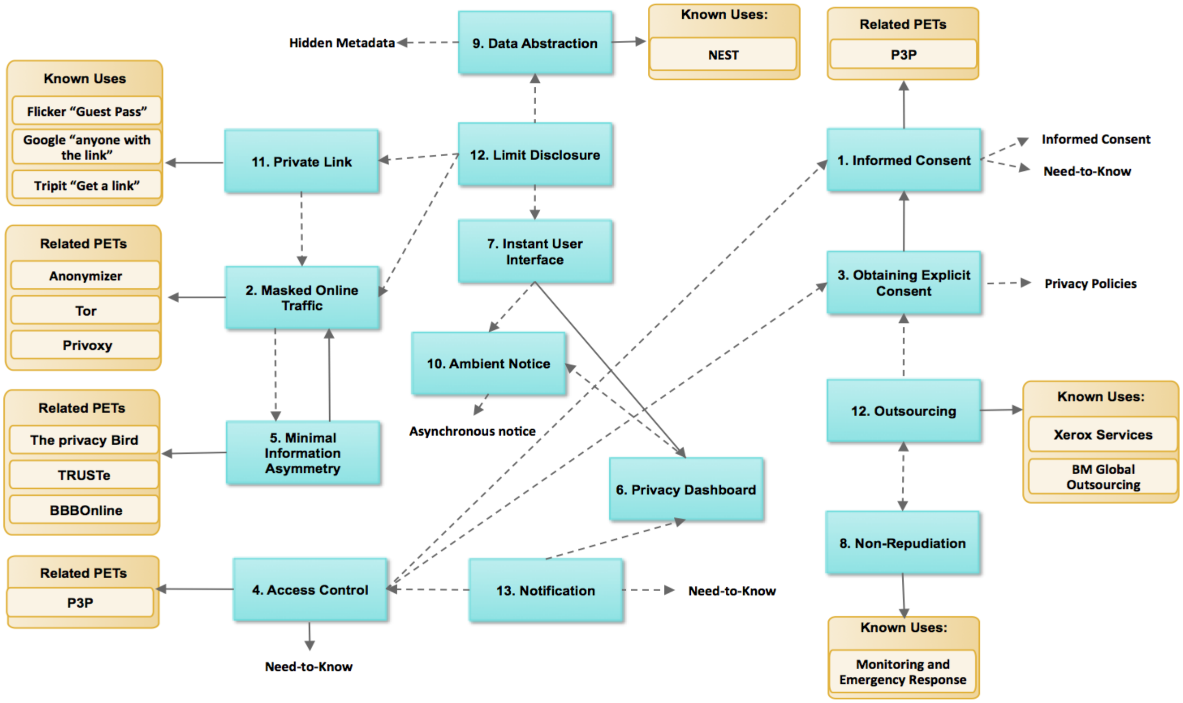


Figure 5. The relationship between the privacy patterns, their known uses and related PETs

4.4 Methodology Model

Nova Scotia's Personal Health Information Act (NSPHIA) was used as a departure point to bridge the compliance gap between the provincial laws. We believe it is going to provide more practical and easier understanding of privacy requirements in the very early design stages at a higher level of abstraction. The process of deriving the proposed privacy patterns relied on both the currently available patterns and the investigation of the legal framework of NSPHIA to cover individuals' rights. Then, the proposed patterns were analyzed against the principles of ISO29100 Privacy Framework and to be used as design guidelines to the next research stage. We believe that the proposed patterns cover all aspects of the NSPHIA and provide a useful guide that should be implemented by any healthcare privacy-preserving system in Nova Scotia even before the design phase and throughout the design lifecycle. The rights according to NSPHIA are as follows: request an access, request a correction, request not to disclose Personal Health Information (PHI), being notified if the PHI is lost, stolen or subject to unauthorized access, request a review of company's decision for access or correction and make a complaint if the custodian did not follow the rules of NSPHIA. The design of the privacy patterns was implemented in the following sequence; designing one privacy pattern for each right; designing privacy patterns for rights that do not have matching or somehow matching patterns; discussing each pattern by explaining the context, problem, proposed solution, and related patterns. The template we followed in forming the proposed privacy patterns was derived from the Pattern-Oriented Software Architecture (POSA2) outline as a simplified version, which was developed by Buschmann et al. (1996).

4.4.1 Justification of the methodology

The currently available privacy patterns that were used and adopted were analyzed and categorized according to the problem from the user (Data Subject) perspective, which are discussed throughout the proposed patterns in Chapter 4. The rest either cover the network or organizational aspects, which is out of the scope of our research. We did not cover the organizations' responsibilities' because there are projects that focus on covering the organization-network perspective: *PrimeLife*[2] project and PReparing Industry to Privacy-by-

[2] PrimeLife project <http://primelife.ercim.eu>

design by supporting its Application in Research project (PRIPARE[3]). They cover the organizational and network aspects with clear organizational goals and architectures. On the contrary, we are interested in the (Data Subject) end user's perspective and UI design, and followed the definition of privacy to help individuals have control over the PI.

We are interested in PHIA compared to other acts because it clearly states and documents the individual rights, which non-legal experts can understand. The other Acts discussed in Section 2.5 focus on privacy requirements in general, and they mix between individuals' rights and organizations' responsibilities which make it not clear for designers and developers who have limited knowledge in privacy legislation to adopt them. As our interest is in privacy patterns from individual rights, we used PHIA as a departure point to bridge the gap between legal language and IT language.

We mapped the proposed patterns to the ISO 29100 Privacy Framework and the Process-Oriented Strategies because they cover the general and worldwide standardizations. We can generalize the patterns by mapping the proposed patterns to these standards-based methodologies. The lack of validation methodologies in privacy patterns is due to the limited number of currently available privacy patterns. The purpose of the mapping besides generalizing the patterns is that we want our patterns not only cover the legal aspect (PHIA) but also international standards. We did not only rely on ISO 29100 principles because we wanted to integrate the legal aspect and be more specific to the individual rights to help them practice their privacy rights.

Therefore, the patterns include both legal requirements and general privacy design requirements. The validation of the revised patterns will be tested in the next phase of the research. This format will aid designers, who are not privacy experts and privacy laws experts, to identify and understand privacy rights in designing the elements of a UI in healthcare systems.

We adopted the format of the POSA2 because it includes all elements that designers and developers need when they search for solutions to solve design problems. A design pattern "provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context." (Buschmann et al., 1996). Following one structure will help designers and envelopers to adopt and use these patterns

[3] PRIPARE project<http://pripareproject.eu>

when they share the same context, problem, and solution: and understand the consequences and challenges they would face. A use case is added when appropriate to explain the flow of interaction between Data Subject as our end user and the UI prototype that implements these patterns. We included the related and similar patterns because we believe that the currently available patterns can be linked for better connections and understanding.

4.5 Proposed Privacy Patterns

Four privacy patterns are proposed to cover the individuals' rights based on NSPHIA. We adopted the classification of the European Directive on Data Protection (2007) and the Italian privacy authority portal (2005) that defined different actors who would be involved in data processing including:

- Data Subject (DS): an individual or a person who has the rights to share, manage and control personal information
- Data Controller (DC): the person who decides in which and how data are processed
- Data Processor (DP): a person or an individual who process data on behalf of the data controller

These definitions were used to identify different roles in the process of proposed solutions to the privacy patterns. The proposed patterns are as following:

4.5.1 Access Pattern

The privacy right assures that individuals have the right to view or receive a copy of their personal health information and fees regarding copying or downloading the PHI might be applied depending on the organization (NSPHIA, 2015).

The proposed flowchart of the privacy pattern is shown in Figure 31 in Appendix A.

Context: Personal Health Information Act (NSPHIA) offers individuals the ability to access their health information in health sector organizations and/or providers including agents.

Problem: Individuals want to use privacy preserving healthcare systems that help to access their personal health information. The individual has the right to have a level of control over the information by gaining access and performing some tasks such as receiving and/or downloading a copy of the PHI record. Individuals have the right to access the privacy policy of the organization or the third party that hosts the information.

Factors: DS: Data subject, DC: Data controller and DP: Data Processor as a third party.

Solution: To design an efficient privacy pattern, we need to provide transparency where DS can access the PHI. PHI is stored within organizations or on external servers. Users will be able to access the PHI and before that, they need to agree on what is saved on these servers according to their rights provided by the NSPHIA. In other words, they will access the information collected about them. As soon as they request access to the information, they need to deal with the consent once and another time after viewing the information to confirm that the information is up-to-date and/or correct and the agreement between the DS and the organization and/or the third party.

Viewing or delivering a copy of PHI should be limited to what the organization can view or deliver to DS based on the time and date was collected.

The following aspects are proposed:

Agreement: The user will be provided with consent in three situations; once to access the sensitive information (PHI) whether the information is stored internally or externally in third parties' servers; the second is to agree on the privacy policy of the third parties with a time stamp[4] because the agreement has to be updated when the privacy policies change; the third is that individuals have to agree on the information stored once they gain access. The individual has the right to opt-out at any time and get a feedback on the consequences to make the most suitable decisions.

Access Control: the user has to clarify the purpose of accessing the information and security measures have to be applied to download the copy, or they can view the document online (i.e. security patterns). This would allow individuals to have a level of control over the information stored about them.

Feedback: the feedback feature should be applied in every pattern to inform and notify individuals of the ongoing changes either in privacy policies or the changes on the PHI.

[4] The time stamp is adopted from the pattern "obtain explicit consent" by Porekar et al. (2008)

Consequences:

The challenge is determining what type of information is collected about them. The EHR of an individual is part of PHI. Is the collected information for research and general health quality or just EHRs that are stored in servers? We will specify the type of information according to the scenario and context while implementing the prototype to be tested to specify the kind of consent that DS has to sign, which depends on the purpose of collecting and the type of information. The purposes to which PHI is collected are included in the design of the proposed Pattern 3. Limiting Disclosure in presenting the list of DCs who are performing activities and the purpose of the activities.

Security assumptions: Secure access and transaction for PHI and Internal audits to ensure compliance for agreements.

Related patterns from literature:

- Access control to sensitive data by Porekar et al. (2008) privacy pattern matches with respect to our individuals having the right to a level of control over the collected information by providing access to the information.
- The privacy pattern known as instant user interface pattern by Bier and Kremple (2012) was designed to allow individuals to understand the reasons for collecting the information by providing feedback and access to the information collected.

4.5.2 Correction Pattern

Individuals have the right to ask to correct any errors in health information. According to NSPHIA, the request should be formally written. If a company rejects the request, the individual has the right to file and submit a complaint to the review officer. It is important to modify the idea and apply it in digital form to serve the ultimate goal of performing privacy patterns that can be considered as guidelines for designing healthcare preserving system. It is considered as a subtask or follow-up task after requesting access to the PHI.

The proposed flowchart of the privacy pattern as shown in Figure 32 in Appendix A

Context: NSPHIA provides individuals the ability to request corrections if the information they gained access is not up to date or not correct.

Problem: Individuals have the right to be able to correct the PHI they have on the system.

Solution: The individual is asked to confirm a consent form that the entered information is correct. Health providers should review the information before approving it and saving it in the database.

> *Agreement:* Individuals have to sign a consent regarding the changes they will make over the stored information. The changes include correcting the currently existing information or adding more information. The consent will save the individuals' rights and record who made the changes and when.
>
> *Review the Changes:* It is the healthcare organization's responsibility to review the changes, confirm them and notify the individual's of the result of the review. Users can track the request and get notified when the review process is complete.
>
> *Feedback:* the feedback feature should be applied in every pattern to inform and notify individuals of the ongoing change on PHI.

Consequences: The proposed pattern applies feedback, access control, and informed consent to be able to complete the request. It is different from the collected information for defined purposes. DS here reviews the accuracy of PHI. The design should clearly separate the type of PHI; one as an EHR and the other as a PHI collected for defined purposes. The context defines the type of the prototype. One exception to the correction is that DS cannot change a professional opinion of health condition.

Security assumptions: Secure access and transaction for PHI from servers.

Related patterns from literature: Access control to sensitive data by Porekar et al. (2008) privacy pattern matches with respect to our individuals having the right to a level of control over the collected information by providing access to the information.

4.5.3 Limit Disclosure Pattern

Individuals have the right to request a record of activities in the form of a list of health agents or providers who accessed the online records and to minimize access to the information. Therefore, the individual has the right to access the information, have a list of who accesses the information, and to limit the individuals who can access the information and/or request not to disclose to certain information.

The proposed flowchart of the privacy pattern as shown in Figure 33 in Appendix A

Context: The DS has the right to get access to a list of activities carried out on their information (have a list of who accessed the information) and can to request not to disclose information (choose from the list).

The pattern is applied in healthcare applications and personal health information. The DS agrees on sharing the information with some health agents and organizations and to limit the access to a well-identified list of agents.

Problem: The DS wants to balance between what is shared and who can gain access. The secondary use of information shared between organizations without consent concerns the DSs.

Solution: By being able to limit the organizations that can access the information the privacy pattern protects DS's health information. It allows for limiting the information shared over organizations as follows:

> *Access Control:* The DS requests a record of activities that have been done on the PHI regarding the list of agents who accessed the information. The DC retrieves the information either from a third party, which should be gained from an earlier agreement or from the organization server. The DS has the ability to: agree on the list, or; limit the list by choosing from the list (blocking some), and request not to disclose at all to any of them. Individuals would be able to choose the information that they decide they would like to reveal and mask the rest by providing levels of disclosure.

Authentication: The system applies two-steps identity clarification technique to lock out unauthorized access and/or modification as a security measure.

Consent: The DSs have to sign a consent on the responsibilities associated with not disclosing information because it is associated with personal health information. The DC has to confirm changes and provide feedback.

Feedback: The feedback feature should be applied to inform and notify DSs of the ongoing changes in case there is a new setting.

Related Patterns:

- The Masked online traffic pattern by (Romanosky et al., 2006) allows users to control what information to reveal and minimize the amount of personal information shared.
- Data abstraction pattern by (Bier & Krempel, 2012) allows individuals to control whom to reveal the information and provide feedback on who has access to the information.
- Private link pattern by (Privacypattern.org) works in limiting who can see the personal health information.
- Instant user Interface by (Bier & Krempel, 2012) allows individuals to opt in or opt out.

Suggestion added to the proposed privacy pattern: Individuals would be able to choose the information that they decide they would like to reveal and mask the rest by providing levels of disclosure.

- Data abstraction pattern by Bier and Kremple (2012) allows individuals to control whom to reveal the information and provide feedback on who has access to the information.

Individuals would be able to choose from a list of agents/health providers and control or decide who can access what**.**

- Private link pattern by Privacypatterns.org (2014) works in limiting who can see the personal health information.
- Instant user Interface by Bier and Kremple (2012) allows individuals to opt in or opt out.

4.5.4 Notification Pattern

> "The custodian is required to notify individuals at the first reasonable opportunity if the custodian believes on a reasonable basis that personal health information was stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and as a result, there is potential for harm or embarrassment to the individuals" (NSPHIA, 2015).

The feedback or notification of the breach should include the following details according to NSPHIA: a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; a description of the types of personal health information that were involved in the breach (e.g., name, date of birth, home address, account number, diagnosis, health card number, etc.); a brief description of what the custodian (Data Controller) is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; any steps the individual should take to protect themselves from potential harm resulting from the breach; and contact information for patients (Data Subjects) to ask questions or learn additional information.

If appropriate, the following information may be included: Recommendations that the individual monitor financial or other accounts; Information about steps the custodian is taking to retrieve the breached information, such as filing a police report (if a suspected theft of personal health information occurred); and Information about steps the custodian is taking to improve security to prevent future similar breaches (NSPHIA, 2015).

The proposed flowchart of the privacy pattern as shown in Figure 34 in Appendix A

Context: The individual under this right is being notified of unauthorized activities performed on his/her personal health information.

Problem: The collected information should be used for the purpose that it was collected for and should not be accessed/and or processed for other purposes. The DS wants to be informed instantly in case of secondary use of information, which includes stolen information, lost or subjected to unauthorized access, use, disclosure, copying, or modification.

Solution: To design a privacy-preserving application, two aspects should be investigated: the system-server aspect and user-system aspect. In case of the system-server, the system should apply the Secure Socket Layer (SSL) to protect it from unauthorized access. In case of the user-system, to prevent unauthorized modification the system should apply two-step identification process.

Notification and consent: The DS is notified in different situations classified according to the type of the practice, which includes; information is stolen or lost as one type, information use, disclosure, copy, and modified as another type. The last type is being subjective to unauthorized access.

Related patterns:

- Need-to-know informs users about recent activities done on the personal health information (Compagna et al., 2009).
- Access control by Porekar et al., (2008) informs users about the requests to access the information.
- Privacy dashboard and ambient notice by Privacypatterns.org (2014) allows users to be informed on how and why the information is collected.

In terms of lost and/or stolen information, the private healthcare system has to notify the DS including the type of data that was breached and associated consequences and apply a further step to increase the privacy and security of the individual by asking to change the password and provide backups that would help in storing information in more secure servers to prevent the consequences of loss or stolen information. The notification has to include ways that the organization (DC) will provide to prevent future breaches (security measures) as well as periodical backups notification with ways for compensation in case of recovery problems. In terms the information was used, disclosed, copied, or modified, the DS will be notified, and the notification should include a list of who accessed indicating if they were third parties and/or healthcare professionals. If a third party performed the privacy breach, a review of the agreement has to be performed, and final notification of the outcome of the review should be provided. In case the breach occurred by a healthcare professional, a regularity body within the organization has to be notified through the proposed pattern. In the case of disclosing the PHI to third parties or health professionals outside Nova Scotia, an agreement should be provided and signed. If the disclosure within Nova Scotia, the Pattern 3: Request not to disclose is proposed.

Regarding being subjected to unauthorized access, the healthcare systems (DC) should prevent the situation before it happens. In case it occurred, the best way to deal with the situation is to notify the individual and apply “system denial.” It can be applied by notifying the DS via email or text message and block access to the record. Applying the two-step authentication reactivates the account.

Security assumptions: Secure Socket Layer (SSL), two-step authentication, system denial, internal audits, and security measures to prevent future breaches.

Consequences: DS is informed about the list of activities and stakeholders who are performing these activities; however, the limit of NSPHIA right is to inform the DS if there is a collection of the information but we think that DS has to agree on collecting the information before the collection with an indication of explicit purposes. A challenge of the pattern is that it does not prevent the unauthorized access before it occurs. We focus on providing feedback when it happens to help the DS make decisions on next steps to recover the breach. We will assume that security measures are already installed from the organizational perspective.

4.6 Validation of the Proposed Privacy Patterns

Because the there is a lack of methods to validate privacy patterns, we evaluate the proposed privacy patterns according to ISO29100 privacy framework and Process Oriented Strategies. Cavoukian (2013) discussed the meaning of accountability in the context of Privacy-by-Design, as it is to use and be able show compliance with design principles and legal requirements. For this stage of research, we focused on showing compliance with design principles and legal aspect; however, clear organizations responsibilities and internal audits should be considered when discussing the accountability of the design (Cavoukian, 2013).

In this section, we validate the coverage of the proposed patterns by mapping them to the ISO 29100 Privacy Framework and Process Oriented Strategies.

4.6.1 The Privacy Principles of ISO 29100

The summary of the ISO 29100 principles is shown in the following table.

#	Principle	Definition
1	Consent and Choice	Present data subject with choices to obtain consent
2	Purpose legitimacy and specification	Insure following legislation and inform data subjects of the purposes to process the PI
3	Collection limitation	Limit the collection of data to the specified purposes
4	Data minimization	Minimize the amount of data collected and the number of actors involved in processing the data.
5	Use, retention and disclosure limitation	Limit the use, retention and disclosure of personal information.
6	Accuracy and quality	Ensure data is accurate, up to date, and relevant Periodically check the data.
7	Openness, transparency and notice	Provide access to information, inform of the policies in place and provide notices whenever there is a change.
8	Individual participation and access	To provide opportunity to access and review personal information
9	Accountability	Inform if there is a privacy breach, apply privacy policy, and provide training.
10	Information security	Provide a level of security by applying protocols.
11	Privacy compliance	The system meets the legal requirements and applies supervision mechanisms.

Table 3. ISO 29100 privacy Framework

The privacy framework was derived from a number of existing principles among countries, states and international organizations (ISO 29100, 2011). There are two main reasons to apply the privacy framework in any Information Communication Technology systems (ICT) in which personal information is processed.

First, the principles should guide the system development in different phases to ensure that the privacy principles are implemented. Second, the framework can be considered as a fundamental model for examining and measuring the privacy-preserving system's performance (ISO 29100, 2011). In some case, there are limited variations in the applicability of the principles due to social, cultural, legal and economic differences, which lead to expectations (ISO 29100, 2011).

We compare each pattern to the ISO 29100 privacy framework to determine whether the proposed patterns cover these principles and what recommendation can be provided to the principles that cannot be mapped. Table 4 provides a summary table of the mapping. We combined the principles (*Purpose legitimacy and Collection limitation*) because they share the same principles.

The mapping process involves dividing the principles into two categories: the covered principles include the mapped patterns while the uncovered include the principles that were not mapped with comments on what we should do about the principles that were not mapped. The coverage of the principle is classified into: ✓ full coverage, ~ partial and × none.

#	ISO 29100 principle		Principle	Coverage	Related patterns
1.	Consent and Choice	1.1	Choices before consent	✓	P1, P2, P3
		1.2	Opt-in consent	✓	P1, P2, P3
		1.3	Inform about individuals rights	×	
		1.4	Individuals should be notified wherever possible	✓	P1, P2, P3, P4, P5
		1.5	Implications of consent opt-out	×	
2.	Purpose legitimacy and Collection limitation	2.1	Purposes to collect information rely on legal base.	~	P3, P4
		2.2	Inform individuals *before* the collection for the first time or for new purposes.	×	
		2.3	Use clear language to communicate the need to process the sensitive data	×	
3.	Data minimization	3.1	Minimize the processing of PI	✓	P3
		3.2	Adoption of "need-to-know" practices	✓	P1, P2, P3, P4
		3.3	Apply techniques to limit linkability by default	×	
4.	Use, retention and disclosure limitation	4.1	Limit the disclosure of information	✓	P3
		4.2	Retain information only as long as defined by the purpose	×	
		4.3	Secure the PI	×	
5.	Accuracy and quality	5.1	Ensure PI is accurate and up-to-date	✓	P2
		5.2	Validate requests to make changes on PI	~	P2

#	ISO 29100 principle		Principle	Coverage	Related patterns
		5.3	Establish control mechanism to periodically check the accuracy of PI	×	
6.	Openness, transparency and notice	6.1	Access to organization policies	✓	P1
		6.2	Notice that information is being processed	✓	P4
		6.3	Provide information about third parties that the information is disclosed to.	✓	P1, P3
		6.4	Notice when major changes occur	✓	P1, P2, P3, P4, P5
		6.5	Offer access, correcting or removing of PI	✓	P1, P2
7.	Individual participation and access	7.1	Ability to access and review	✓	P1
		7.2	Allow to access, correct and remove	✓	P2
		7.3	Information about the changes and the third parties	✓	P1, P3
		7.4	Apply procedures to practice these rights	✓	P1, P2, P3, P4, P5
8.	Accountability	8.1	Documentation of the privacy-related policies	~	P1
		8.2	Assign an internal person to implement the privacy-related policies	×	
		8.3	Privacy policy of third parties with the same level of protection	✓	P1, P2
		8.4	Inform individuals about the privacy breach	✓	P4
		8.5	Procedures for compensation in case was difficult to recover the privacy of an individual	×	
9.	Information security	9.1	Mechanisms to protect from unauthorized access, use, disclose or loss	×	
		9.2	Provide organizational, physical and technical controls	×	
		9.3	Risk assessment and audit processes	×	

#	ISO 29100 principle		Principle	Coverage	Related patterns
		9.4	Implementing these control to mitigate consequences of the privacy breach	~	P4
		9.5	Limiting access to PI	✓	P3
10.	Privacy compliance	10.1	Internal mechanisms to ensure compliance with relevant law	~	P1, P2, P3, P4, P5
		10.2	Develop a privacy risk assessment to evaluate the service complies the data protection and privacy requirements	×	

Table 4. Summary table of mapping principles

4.6.1.1 Covered Principles

Consent and Choice principle includes: principles 1.1 (*choices before consent*) 1.2 (*opt-in consent*) and 1.4 (*individuals should be notified wherever possible*). Principles 1.1 and 1.2 are applied in the proposed patterns: *P1 (access pattern), P2 (correction pattern) and P3 (limiting disclosure)* since presenting individuals with available choices and consent is the primary task accomplished by these patterns. For example, in terms of *P1 (access patterns*), there are three types of consents one is to agree on the type of information stored or collected internally and what information stored externally in third party's servers. The DS provides an agreement according to the presented choices. If the PHI is stored internally, the DC presents the DS with the organization's privacy policy and provides the DS with consent to sign. If the PHI is stored externally, the DS has to perform an agreement on the DP privacy policy. In terms of *P2* (*correction pattern),* DC provides the individual with consent regarding the correction and the responsibility of updating the stored information.

P4 (notification pattern) covers the principles 1.1 and 1.2 by providing the individual with choices on further steps taken to preserve the privacy and consent to apply the choices. For example, in case of stolen and lost PHI, the DC provides the DS with choices to mitigate the risk by both changing passwords and gaining agreement to backup the PHI. The principle 1.4 individuals should be notified wherever possible is applied in all patterns after consents and major changes occur.

Purpose Specification and *Collection Limitation* are intended to define the need for data minimization. However, the aspect of ensuring that the purpose to collection information is accepted and relies on legal base (i.e., clear purpose, retention time and agreed on) is achieved from the first steps of design because we proposed our privacy patterns in accord with the legal framework of NSPHIA. The individual rights rely on giving the user feedback on reasons for collecting the information and request a list of activities done on the information, which is part of *P3* (*limiting disclosure)* and *P4 (notification pattern)* and mapped to the principle 2.1. The notification should include: purpose of collection, purpose comply with law, consent to opt-in and opt-out.

Data minimization and use, retention and disclosure limitation principles are intended to limit the use of collected information as primary tasks; however, they can be mapped to the pattern *request not to disclose information* for principles *3.1* minimize the processing of PI and 4.1 limit the disclosure of information by providing the DS with a list of activities on the PHI and allow DS to limit the list by choosing not to disclose the information. Therefore, the DS has the opportunity to agree on the list of stakeholders who can access; limit the list by choosing from the list (blocking some); and request not to disclose at all to any of them, which lead to minimize the processed data from the DS aspect. The principle 3.2 adoption of "need-to-know" is applied by all five patterns because they provide feedback whenever a change occur such as the agreements on consents, accepting requests, confirmation. For example, the principle 3.2 can be applied in *P4 notification* by informing if the PHI is lost, stolen or subject to unauthorized access.

Accuracy and quality principle includes 5.1 (*ensure PI is accurate and up-to-date*), and 5.2 (*validate requests to make changes on PI*) that are applied in P2 . The DS is able to review the accuracy of the PHI and make changes to the stored PHI. After making the changes, the DC has to validate the request before storing the PHI.

Openness, transparency and notice and *Individual participation* principles are overlapped and share some aspects. The principle 6.1 (*access to organization policy*) is implemented by P1 (*request an access*). The DS is presented with the organization policy and third-parties policies. The principles6.2 is mapped to the P4 provides a feedback notice to the DS if information is information is being used, disclosed, copied and modified.

The principles 6.3 and 7.3 are about providing information of third parties that the PI is disclosed to which the P1 provides when DS accesses and review the policies and *P3* provides the DS with a list of third parties who access the PI with the ability to apply changes to the list.

All patterns are mapped to the principle 6.4 because of the feedback provided whenever there is a change on the PHI. Principles 6.5, 7.1 and 7.2 ensure the ability to access, review and remove PI which *P1 (access pattern)* and *P2 (correction pattern)* are mapped. The principle 7.4 applies procedures to practice these rights in principle (*Individual participation)* matches what we are proposing by minimizing the gap between individuals' rights and integrating these rights as design requirements to endure compliance.

Accountability principle ensures that third parties offer the same level of protection of the organization in 8.3. The DS can access and the third-party policies which is mapped by P1 and P2. The principle 8.4 (*inform individuals about the privacy breach*) is mapped by *P4 (notification pattern).*

The principle *(information security)* includes principle 9.4 (*implementing controls to mitigate consequences of the privacy breach*). P4 (*notification pattern)* is taking the DS to further steps to some extent in dealing with situations of privacy breach. For example, system denial and backing up the PH are proposed; however, if it is difficult to recover form privacy breach, it is the organization responsibility to apply procedure or compensations. The principle 9.5 (*limiting access to PI*) is mapped to the P3 (*limiting disclosure*) while DS has the opportunity to limit the stakeholders who can access and apply changes to the list.

The principle *Privacy Compliance* is mapped through all five patterns because the patterns were designed in accord with the rules of NSPHIA by the principle 10.1 (*internal mechanisms to ensure compliance with relevant law*).

4.6.1.2 Uncovered principles

The uncovered principles are the ones that were not mapped. The question is: what we can do to the principles that were not mapped. To answer the question, a discussion of each uncovered principle along with a suggestion either to the patterns or if they are out of the scope is as follows:

Consent and Choice principle includes principles that were not mapped: 1.3 (*inform about individuals' rights*) and 1.5 (*implications of consent opt-out*). In terms of the principle 1.3, the patterns propose design guidelines to implement the rights but not informing the DSs about their rights related to their PI. A suggestion would be adding “the inform” of the individuals’ rights as a fourth point to the P4: *notification pattern* by providing the DS with a documentation about their rights in accord with NSPHIA as reference and a reminder.

In terms of principle 1.5 the implications of consent opt-out was difficult to map because the limits of the rights under NSPHIA is to gain consent on collecting PHI and be informed about who processes the PHI. Therefore, the consequences from opting out from the consent would or would not make a change in processing the PHI is not clear from NSPHIA rules perspective. By applying P3 (*limiting disclosure)*, DS can have a list of stakeholders or agents who are processing the information and can limit them; however, the DS needs to have a feedback of consequences applied before choosing to opt out such as a full description of the cut down of health benefits regarding better diagnose or keeping track of latest health solutions. A suggestion would be adding a feedback with details about consequences of opting out while blocking.

The principles *(Purpose Specification)* and (*Collection Limitation)* include: 2.2 (*inform individuals* ***before*** *the collection for the first time or for new purposes*). The rights in accord with NSPHIA include consent opt-in, inform while processing, who is processing the PHI but indicating the reasons or purposes to collect the PHI is one of the organizations’ responsibilities but not informing before collecting the PHI. To map this aspect, we can add it as a fifth inform point to pattern P4 (*notification pattern)* as a suggestion and both the pattern and this aspect are based on “inform”. The principle 2.3 (*use clear language to communicate the need to process the sensitive data*) is part of prototype for the next phase of the research by designing HCI-related aspects regarding the UI of the prototype, which include: *Interaction* (steps takes to support the flow of interaction i.e. steps of access, correction, and feedback), *Consent* and *Policies* representation and wording, *Visualization* including notices, feedback, and privacy icons, and privacy Dashboard for displaying the rights and settings.

The principle (*Data minimization)* includes the principle *3.3 (apply techniques to limit linkability by default*) that was not covered by the proposed patterns. A suggestion would be following one the proposed patterns by Hafiz (2006) and the patterns are designed to cover the technical-network side and has a collection of patterns to apply minimization by default; however, it is out of the scope in this stage of work.

The principle *(Use, retention and disclosure limitation* include 4.2 (retain information as long as defined by the purpose) is not covered by would be added to *P4 (notification pattern).* The notification should include the time the information will be retained along with the other details such as purpose of collection, purpose comply with law, consent to opt-in and opt-out. The principle 4.3 (*secure the PI*) is not mapped because it is out of the scope due to security-technical-network patterns that have to be applied. At this stage of work we assume that these security patterns are already implemented and discussed the related security measures that are needed in each proposed pattern.

Accuracy and quality was not mapped for the principle *5.3 (establish control mechanism to periodically check the accuracy of PI*). It is one of the organizations' responsibilities according to NSPHIA; however, P1 (*access pattern)* and P2 (*correction pattern)* allow the DS to have some level of control by accessing and checking the accuracy of the PHI. The principle focuses on the organization side not the individual side, for which reasons it cannot be mapped.

Accountability is not mapped to our patterns because it focuses on assigning a person to check periodically the organization practices in principle 8.2 while 8.5 focuses on applying procedures for compensation in case was difficult to recover the privacy breach. This step is the organization responsibility because the individual rights are limited to inform the DS in case of the privacy breach; However, the procedures can be added to the documentation of the privacy policy and be part of the P4: being notified along with purposes and collections details before starting the collection.

Information security includes *9.1 (mechanisms to protect from unauthorized access, use, disclose or loss*). The rights under NSPHIA ensure informing the DS whenever there is a breach; however, the proposed patterns do not cover the protection before the breach and it is the organization's responsibility to implement security patterns that use proxies or other protection techniques. The principles *9.2* and *9.3* focus on providing the technical controls and provide risk assessment. These principles are out of the scope due to the lack of the context regarding the risk assessment and risks associated with the patterns: however, we believe that NSPHIA was built to overcome privacy risks. A suggestion would be performing a risk assessment after implementing the prototype and before testing it with end-users. The risk assessment is included in the *Privacy compliance* principle*,* which is not mapped to our patterns for the same reason.

The comparison of the proposed patterns with the ISO29100 principles showed that there is an overlap between some principles such as consent and choice, and purpose specification. Collection limitation and data minimization share quite the same principles.

4.6.2 Process-Oriented Strategies or Privacy-By-Policy

The process-oriented strategies (Hoepman, 2014) were built on top of the privacy-by-policy approach designed by Spiekermann & Cranor (2009). The approach relies on providing notice and choice principles while processing personal information and focus on the individuals more that than architecture or organization-network perspective. Because it focuses on individuals, we aimed to map the proposed patterns to the Process-Oriented Strategies. The strategies are summarized in the following Table 5.

Strategy	**Definition**
Inform	Data subjects should be adequately informed whenever personal data is processed
Control	Data subjects should be provided agency over the processing of their personal data.
Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced
Demonstrate	Be able to demonstrate compliance with the privacy policy and any applicable legal requirements

Table 5. The process-oriented strategies by Hoepman (2014)

The *inform* strategy states that individuals should have the opportunity to be informed about reasons for processing the PI and the Information being processed. The strategy can be mapped by the P3 (*limiting disclosure). The DS* is informed about the purpose of collection, consent to opt-in and opt-out. The strategy supports informing DSs about their rights to access the PI which can be added as a suggestion in the P3 (*limiting disclosure)* by providing the DS with documentation about the rights in accord with NSPHIA as reference and a reminder. The aspect can be linked to the principle 1.3 from the ISO 29100 as not covered principle.

The *control* strategy focuses on providing the DS with a level of control over their information. The patterns P1 (*access pattern)* P2 (*correction pattern)* and P3 (*limiting disclosure)* are mapped to the strategy. By applying these patterns, DS are able to access, correct, check accuracy and receive a list of “who” access the PHI. The DS can make changes to the list by blocking and limiting the disclosure of the PHI and have the ability to have a pre-defined list.

The *enforce* strategy ensure the ability to access the third-parties policy regarding the collection and the storage of information, which is proposed in P1 and P2. The DS has the right to access the third parties policies and sign an agreement. The *demonstrate* strategy ensures that the privacy policies is enforced by applying the logging and auditing mechanisms which is out of the scope of the stage of work.

5 Chapter 5: Phase Two: Interview Study and Requirement Gathering Phase

5.1 Introduction

There are a variety of techniques used to gather design requirement include questionnaires, interviews, observation, prototyping (Hoffer et al., 2011). In this Chapter, the primary focus is on applying in-depth interviewing as a methodology to develop privacy-preserving design guidelines based on NSPHIA as a case to represent privacy laws. The participatory design perspective is covered by interviewing different stakeholders who are NSPHIA users and are required to show compliance with NSPHIA.

5.2 Related Work

5.2.1 What is In-depth Interviewing?

Participatory Design (PD), as the general theme of the project, is a mixed method approach where many research approaches can be applied. For this stage of our project, we are focusing on interviews, particularly In-Depth Interviews (Guion et al., 2001). In-depth Interviewing is "a qualitative research technique that involves conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular idea, program, or situation" (Boyce & Neale, 2006, p. 3).

Focus groups and in-depth interviews are considered to be the most common methods used in qualitative research, and they share some advantages such as the rich information and the low in cost, which are difficult to achieve from surveys and other quantitative methods (Milena et al., 2008).

However, in-depth interviewing is showing a higher level of success in exploring and gaining a deeper understanding of sensitive topics that participants may be stressed or hesitated to discuss in a group as indicated by the study conducted by Milena et al. (2008).

5.2.2 In-depth Interview as a Requirement Gathering Approach

The In-depth interviewing has been applied in a variety of research purposes. In-depth interviews can be used to develop guidelines such as in Milewski & Parra (2011) who have conducted a study to answer the research question: how people use health information to manage chronic illness. They used the qualitative data they gathered to create a set of formative requirements to support the design of personal health management systems.

In-depth interviews can be used to understand barriers of a case. In Latulipe et al. (2015), researchers have conducted in-depth interviews to investigate the reasons behind the current barriers regarding patient portals adoption among older adults in rural populations. Based on the results, they created a set of considerations to help healthcare clinics to design patient portals that are based on patients' experience.

They can be deployed in case of exploring a research idea for in-depth analysis and provide prototyping guidelines. Solomon et al. (2016) adopted an iterative user-centered design process that includes in-depth interviews as a method to get detailed feedback on the proposed prototypes for better representation of test results in online portals. It is an appropriate method to gather requirements based on user experience as suggested by Mannonen et al. (2014). A different type of interviews was conducted which is decision-making method (CDM) to provide a detailed description of work experiences. In-depth interviews were conducted to understand the challenges that different stakeholders face in using Electronic Medical Records (EMRs) by Terry et al. (2014).

In our case, we need to gain in-depth information from different knowledgeable stakeholders who are considered as NSPHIA users and required to show compliance with NSPHIA rules. We are interested in their experiences that result from their involvement in the process of meeting with NSPHIA rules and the current practices in the management of Personal Health Information (PHI).

5.2.3 Current Healthcare Systems in Nova Scotia and MyHealthNS

Prior to interviewing stakeholders who are involved in the process of complying with NSPHIA, we wanted to conduct a review of the current healthcare systems in Nova Scotia where NSPHIA is applied. In doing so, we could base our research on a real case where our contributions can benefit, shed light on how PHI is managed, and the proposed user interface design guidelines can be applied.

We found that the province has an EHR called SHARE and three recommended systems by the Department of Health and Wellness (Department of Family Practice, 2017). Further, we found that only these EMRs can connect to other portals such as lab results and diagnosis

(Agency for Healthcare Research and Quality, 2017). They are Nightingale On Demand ASP[5], Practimax[6], QHR Accuro ASP[7] and Personal Health Records (PHRs) in the form of the online portal MyHealthNS (Health and Wellness, 2016). According to HealthIT (2013), a PHR is an online application that is used by patients to keep and supervise their health information in a confidential, private and secure, environment.

MyHealthNS[8] is an example of a PHR that allows patients to receive, view and manage their personal health information electronically, making it more convenient. The goal of the project is “introduce a new e-health solution to the provincial healthcare system” and “to facilitate self-managed care” (Health and Wellness, 2016). We reviewed MyHealthNS to be able to relate our contributions to a real case by proposing design guidelines to the user interface of the online portal based on NSPHIA as a privacy law.

5.3 Research Objectives and Questions

The main objective of the interview study is to form privacy-preserving design guidelines that cover NSPHIA rules. Another goal is to take the first step toward bridging the gap between IT designers and legal representatives by collecting qualitative data from different stakeholders to draw a complete picture of current practices, challenges, knowledge, experience, perception and future recommendations on managing PHI in general and through online portals. For better understanding and exploration, we need to cover the following technological, managerial and legal perspectives:

5.3.1 Technological and Managerial Perspectives

The research questions cover aspects of:

- How is Personal Health Information (PHI) collected and used, what are the secondary uses, and what are the breach notifications / consents from a legal perspective?
- What are the reasons behind the compliance gap?
- What technology considerations should be made to comply with privacy laws in general and NSPHIA in particular?
- How should designers comply with privacy laws? What legal consequences are associated with not complying?

[5] http://www.nightingalemd.ca
[6] http://practimax.ca
[7] http://www.qhrtechnologies.com
[8] https://www.myhealthns.ca

5.3.2 The Legal Perspective

The research questions cover the following aspects:

- How are Electronic Health Records (EHRs) managed in local-based healthcare systems and through online portals, and what are the associated challenges?
- What forms of compliance are followed with privacy laws in general and Personal Health Information Act (NSPHIA)?
- How is privacy maintained in current practices?

5.4 The Research Methodology

5.4.1 Study Process

In our quest to develop privacy-preserving design guidelines, the process of designing the study by conducting in-depth interviews underwent five main stages: *Thematizing*, *Designing*, *Interviewing*, *Analyzing*, and *Proposing* as shown in Figure 6.

5.4.1.1 Thematizing

The *Thematizing* stage relied mainly on the analysis of patients' privacy rights under NSPHIA. The analysis focused on providing a detailed understanding of each patient's privacy rights under NSPHIA. Privacy patterns were proposed to cover privacy rights and organization responsibilities from the previous research stage (Phase One in Chapter 4). We formed the research questions and underlined the gaps resulting from the analysis of NSPHIA and privacy patterns. These gaps were caused by the interdisciplinary nature of the context.

Specifically, we covered NSPHIA as follows: privacy legislation from a legal perspective; a design guideline from a technological perspective; and how PHI is managed from an administration perspective. Gaining feedback from all stakeholders who are representatives of these disciplines was vital for our study. Therefore, the result of the *Thematizing* phase is a set of categories and aspects that synthesize both NSPHIA rules and privacy patterns as shown in Figure 7. *Thematizing* is performed after determining which target stakeholders have a direct or indirect influence on the study process.

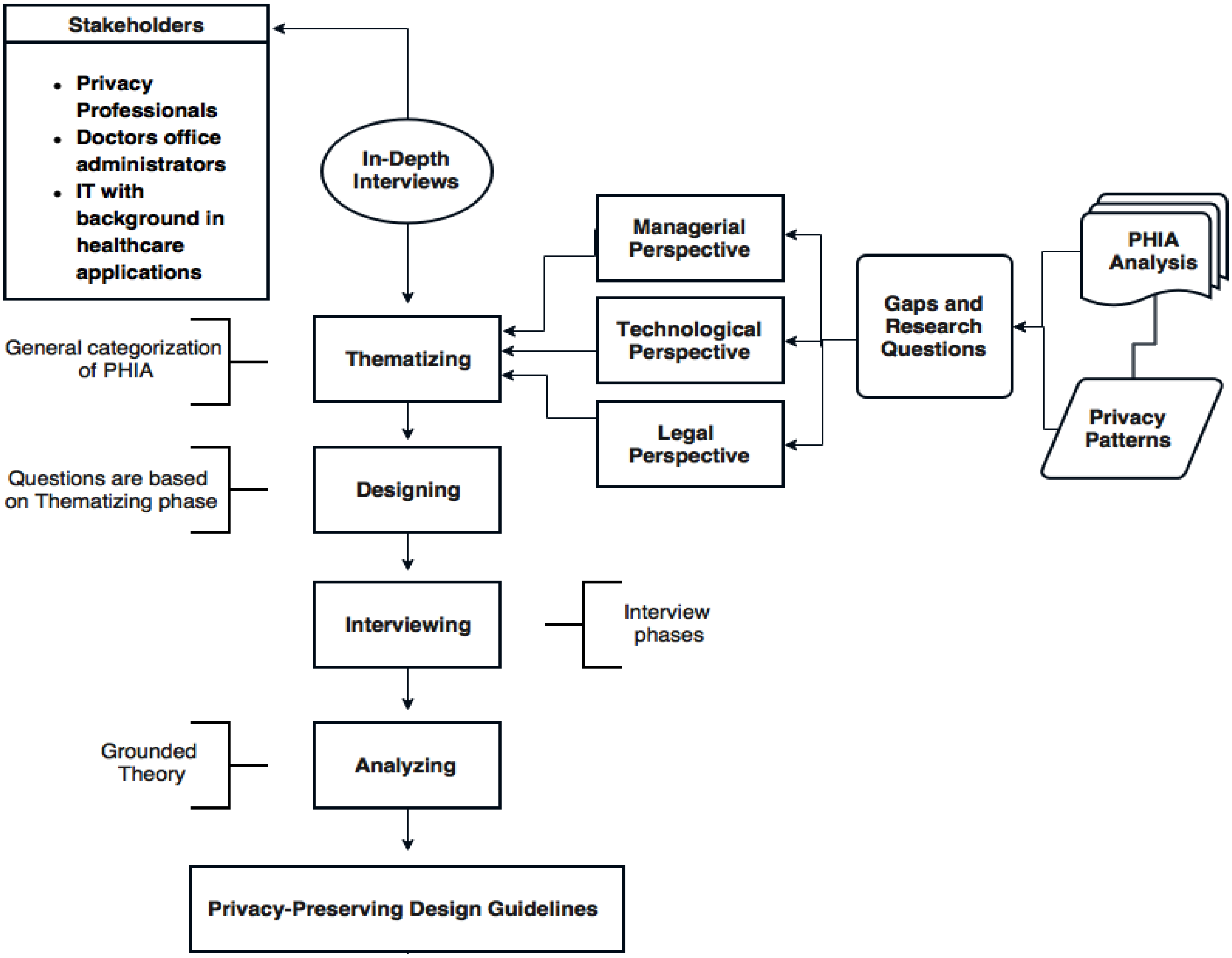

Stakeholders
Privacy Professionals
Doctors office administrators
IT with background in healthcare applications
In-Depth Interviews
Managerial Perspective
Technological Perspective
Legal Perspective
Gaps and Research Questions
PHIA Analysis
Privacy Patterns
General categorization of PHIA
Thematizing
Questions are based on Thematizing phase
Designing
Interviewing
Interview phases
Grounded Theory
Analyzing
Privacy-Preserving Design Guidelines

Figure 6. In-depth interviewing methodology model

5.4.1.2 Designing

The interview questions are based on the general categorization from the *Thematizing* phase. The questions for privacy law representatives fall under the categories of: (a) data access, consent, data collection; (b) notification; and (c) privacy preferences. We then added to these categories current practices, challenges, knowledge, experience, perception and future recommendations for managing PHI in general and through online portals to IT employees and administrators in physicians' offices in particular. Throughout our study, we explore their basic practices, what did they do in the introduction of NSPHIA, and what has changed in their practices.

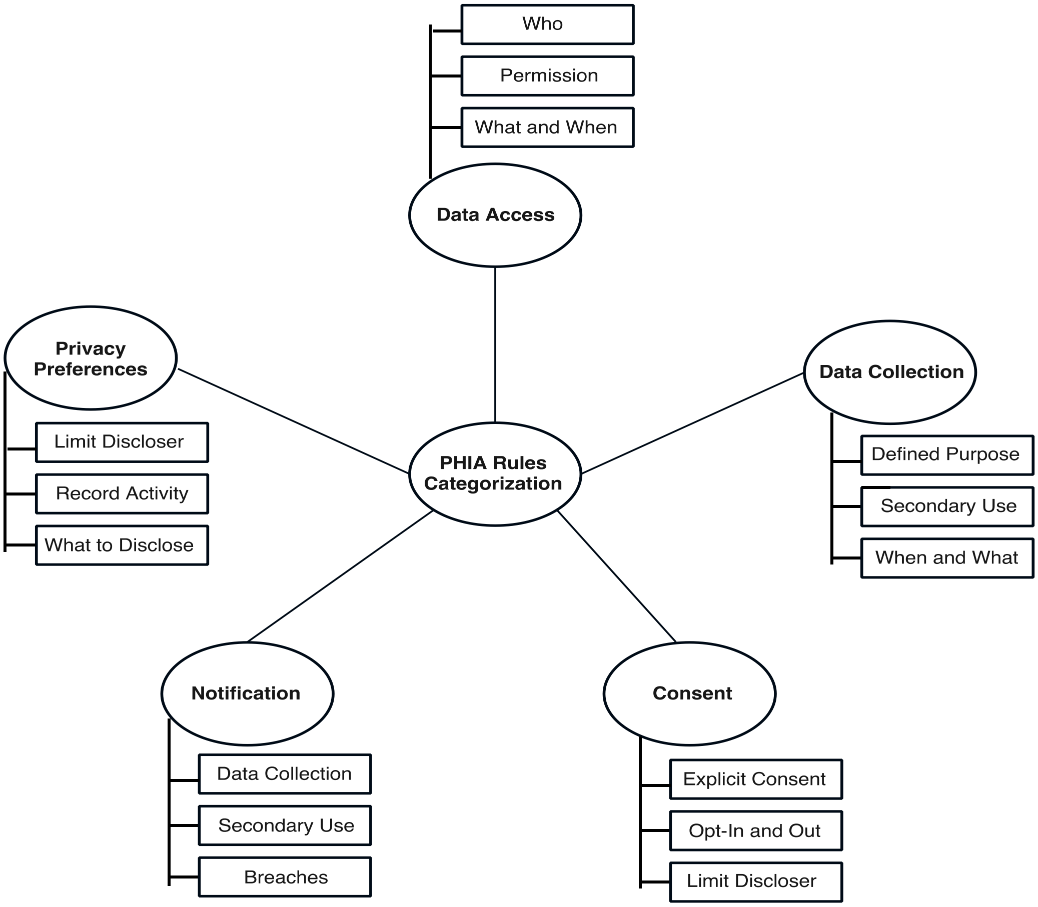


Figure 7. NSPHIA rules categorization

5.4.1.3 Interviewing

The flow of an in-depth interview goes through many phases, as adopted from (Maguire, 1987). It starts with the "nurturing" phase, which aims to provide the participant with an introduction to the study, as well as a quick review of the study objectives and answers to the background questionnaire. The background questionnaire covers participants' demographic information and the type of system they are using, along with a self-perceived description of their level of experience.

The "energizing" phase aims to talk about the general problems and the research gap that we are trying to bridge. In the "body" of the interview phase, the investigator managed the asking and probing interview questions necessary to address the main objectives.

The final phase starts with the "closing", where the investigator summarizes some important points and the participants are thanked for taking the time to participate. The penultimate phase to proposing the privacy preserving design guidelines is using grounded theory as an analysis method.

We are planning to probe when it is appropriate for more details. Interviews are an effective method for probing to find answers “beneath the surface, soliciting detail and providing a holistic understanding of the interviewee’s point of view” (Patton, 1987, p. 108; Cataldi, 2018).

5.4.2 Participants and Data Collection

We recruited participants who maximized the reliability and validity of the study outcomes by choosing who we consider to be good sources of information due to their experience and knowledge (Miller et al., 2016). The population of the study includes different stakeholders who are NSPHIA users and residents of Nova Scotia. They were recruited through: (1) the university faculties (Law, Information Management and Health Informatics, and Computer Science; and (2) an advertisement in the weekly newsletter of the http://www.doctorsns.com website to reach medical office administrators along with the following:

- Information technology (IT) employees with background and experience in healthcare systems and Health Informatics;
- Physicians’ office administators, regardless of IT background; and
- Privacy Professionals who have experience in both Health Information Systems and Privacy Legislation in Canada.

The researchers received training in conducting interviews and piloted the study to refine the interview questions. During the first interview, we followed the interview guide. However, the probes were made according to the participants’ answers, aiming to seek examples or more in-depth information. The interviews lasted from 45 to 60 minutes and were audio-recorded for analysis purposes. The confidentiality of the recordings and participants’ information was maintained.

Data collection included interview answers with different target populations, observation notes made throughout the interviews, and memos. We interviewed four doctor’s office administrators, two privacy professionals, and two IT healthcare employees. Participants’ demographics, showing their education level and experience in years, are shown in Table 6.

We faced some challenges in recruiting privacy professionals and legal consultants[9]. The intended number of participants as a sample size was from 25 to 30. In dealing with the

[9] Data privacy officers hard to find in Nova Scotia. Jan. 2018. Retrieved: From:http://www.cbc.ca/news/canada/nova-scotia/data-privacy-nova-scotia-officer-business-1.4505910

challenges in the recruitment process, we had to extend the time for data collection from six months to one year.

A few of these challenges are detailed as follows. First, we experienced difficulties recruiting NSPHIA representatives from the NS Department of Health and Wellness. We wanted to collect qualitative data on the process of designing privacy rules and filling the gap that resulted from our initial analysis. The original plan was to cover the legal perspective by interviewing whoever designed NSPHIA as NSPHIA representatives; however, the lack of interest in participating in our study was an unexpected a barrier. We then thought of local privacy professionals as a source of information, as they have experience in both health information systems and privacy legislation. One of the privacy professionals we interviewed is a committee member who helped design NSPHIA.

Secondly, some of the participants who contacted me immediately did not meet the eligibility criteria, such as minimum years of experience (i.e., 2 years). Three office administrators never returned our invitation after the first notice of participation interest. However, the eight who did respond provided sufficiently robust data for this study. Two researchers reviewed the interviews, emerged categories from the data analysis, and agreed that the data included covered the main aspects of the research questions.

Participant ID	**Gender**	**Education Level**	**Experience (in years)**	**Position Title**
Admin 1	Male	Bachelors	2	Medical Office Administartor
Admin 2	Female	Bachelors	12	Administartive Assistant
Admin 3	Female	Bachelors	9	Medical Office Administartor
Admin 4	Female	Bachelors	15	Medical Office Manager
Privacy Professional PP1	Female	Master’s Degree	27	Legal Consultatnt
Privacy Professional PP2	Female	Doctoral Degree	25	Assistant Professor
IT Specialist 1	Male	Doctoral Degree	10	Assistant Professor
IT Specialist 2	Male	Bachelors	6	EMR Adisor

Table 6. Participants' demographic information

Interviewing the Privacy Professionals and IT Specialists along with experienced Medical Office Administrators was vital in the current research phase (i.e., the requirement-gathering phase) as the reliable departure point.

5.4.3 Refining the Interview Guide

The interview guide is developed based on the gaps we found in the Thematizing stage. I piloted the interview questions once, and questions were refined. I reflect on some points during the interviews and the process of refining the interview questions (Appendix C).

During the first interview, we followed the interview guide. However, the probes were made according to the participants' answers, aiming to seek examples or more in-depth information. I had the situation that the participant keeps saying I do not know. What I did to get more answers is I tried to create scenarios of each point and look at if they had the same situation or what they would do if they have such conditions. Scenarios helped us allowing a discussion, but it might limit their answers to only these situations. An example is the question number 4. Instead of asking "what type of access to patients PHI is considered as unauthorized access?", I asked in the form of scenario as following: "let's say that you had received PHI in any form "imaging or blood work with patients identifying information" and you realized that information does not belong to any of the patients who are seen by the doctor" and then I start probing: what would you do? What next steps would you take? Is the patient notified? Why and why not? What other cases that they are considered as unauthorized access? I adjusted some of the interview questions to focus more on the areas that needed clarification and used for probing during the interview.

5.4.4 Justification of the Methodology

We have applied the in-depth interviewing method for several reasons. First, "the research method of in-depth interviewing is used to learn [about] the individual perspectives of one or a few narrowly defined themes" (Brounéus, 2011). Reflecting on our study, the general categorization in the *Thematizing* stage resulted informing five themes that cover managerial, technological and legal perspectives that interview should focus on as supported by Brounéus (2011). We applied it to gain deep feedback to understand the current practices as enforcing an emerging (new) privacy law might face some challenges as narrowed themes. These themes will guide the discussion; however, each interview will take its twists according to the interviewee answers (Brounéus, 2011).

Second, it helps obtain depth detailed data about an issue directly from ‘knowledgeable’ participants (Wallace Foundation, 2017 & Boyce and Neale, 2006, & USAID, 1996), and it is faster to gain information than other observational methods (Maguire et al., 1998). It is recommended when the research has a short timeline, and the study participants are difficult to be recruited (Wallace Foundation, 2017; Turner, 2010; Mack et al., 2011; Alshenqeeti, 2014). According to Coombes et al. (2009), an important advantage of IDI is that the priority is given to the participants. Those participants are chosen because they have knowledge and experience and the flexibility of the process of asking and probing would enhance the validity of the findings (Coombes et al., 2009).

Third, applying the method of in-depth interviewing has shown significant advantages in different development phases of the design life cycle (USAID, 1996). However, in-depth interviewing should be applied in the initial stage of research due to the richness of the information that can be collected (Turner, 2010; Mack et al., 2011; Alshenqeeti, 2014). Then, the research can have a defined path to follow. We planned to conduct the in-depth interviews at the early stage of our research to have a clear path to follow for next research steps.

5.4.5 Grounded Theory as an Analysis Approach

We use a combination of paper annotations and *ATLAS.ti* software to analyze the interview scripts. We adopted the two phases of the grounded theory as analysis process.

5.4.5.1 Initial Coding

Initial coding is applying word-by-word and line-by-line coding. In our study, the coding process started with looking at each question and coding each response, and then I moved to the next question until all the interview questions were coded. I tried to assign analytic and straightforward codes to describe the parts best. I listed all initials codes according to the participant’s ID in a table and checked how frequent the codes were assigned.

We had vast numbers of initial codes in each interview. Initially, I used *ATLAS ti.*7 software to manage all these codes. Then, we compared between these codes after each interview coding and re-coded these initial codes to be sure that we had clear codes that represented each interview before moving on to the next step of coding. In this stage of analysis, we recognized that there were gaps that lead me to ask more questions of the data itself. Then, we focused on these gaps throughout the interviews that followed.

According to Charmaz (2014), researchers could use line-by-line or incident-to-incident coding based on the type of data they collect. In my study, which seeks a deeper understanding of the current practice in managing PHI, we used both line-by-line and incident-by-incident coding to help me capture the dimensions and properties of each emerging code and category.

5.4.5.2 Focused or Selective Coding

Charmaz (2014) stated that "focused coding means using the most significant and frequent earlier codes to sift through large amounts of data … [and that it] requires decisions about which initial codes make the most analytic sense to categorize data incisively and completely". In this phase, we focused on the incident-by-incident coding process, which includes performing comparisons to outline the similarities and differences within the code category (Charmaz, 2006). It is a [conceptual selection] of the initial codes to categorize them to the most significant code category that best fits the context. It is not a linear process because I was going back and forth to match and reorganize and relink the categories and their codes along with reading the interview scripts for many times. It is a complicated process because I had some codes that are linked to more than one code category and some codes that can be listed in many categories. I had to read the interview scripts for the last time to assign the code to the most significant category by applying an ongoing interaction with the interview scripts.

This list resulted from the initial coding was revised for three times as follows:

1. The first revision is to rename and remove duplicate codes or if some codes share the same meaning.
2. The second revision is to merge and classify codes according to the links between them.
3. The third revision is to link code categories/groups according to the relationships between them.

The code categories and the sub-codes resulted form the analysis process are included in Appendix B.

5.5 Results and Discussion

The purpose of this study is to explore and understand the current practices in managing Personal Health Information in Nova Scotia and NSPHIA compliance. Therefore, this section represents the findings that emerged from the data analysis of participants.

5.5.1 Privacy-Preserving Framework to Comply with Privacy Legislation Including Design Guidelines for User Interface

The framework entitled "Privacy-Preserving Design Guidelines to Comply with Privacy Legislation in Online Patient Portals" reflects the main categories and design consideration need to be covered during the design phase of privacy-preserving PHI technology, which is an online portal in our case. The framework fit in the context of EMR that is connected to the PHR or the online portal and is managed by the physicians' office administrators and patients. The themes derived from the interview study that consists the framework include:

5.5.1.1 Access

The concept access was covered from different perspectives during the interviews and divided as follows (as shown in Figure 35 in Appendix B):

Who can access the patient information?

From admins points of view only the office administrators and the physicians who can access patient data or the medical records. Some admins stated that others can have access such as registration clerks, clinical staff and practitioner nurses, office managers, surgeons, and MSI [Nova Scotia's health insurance program: Medical Services Insurance] for billing purposes.

Admin 2 said:

> "They will only be able to receive information for patients that they would have their hospital number."

It is the case where the practice is a part of a larger hospital and they use both paper and electronic records.

Physicians' Access:

Physicians can exchange patient information, and it is accessible because they will either ask for patient information or receive them through fax or email. However, in current practice, EMR systems do not talk to each other [physically not connected].

Admin 1 said:

> "It is smart to have direct contact between physicians for the purposes of treating the patients. It is smart, and it is more efficient. I have no idea about the cost, but this is not yet done in current practices. If the information is online, it is an immediate access."

Admin 4 supported what Admin 1 said because of the current setting of the clinics in Truro. More than one physician is working in the same place and they cover for each other's:

> "These systems do not talk to each other which would be much way better if there is pair set up if they could, and they are kind of waiting to see what [the telecommunications company] TELUS can bring out because all the doctors in Truro areas they are already now in something other than Nightingale. They want to could access everybody because they cover for each other and so it would be much easier for them to be able to do that and get access to patients' information when they are covering on the weekends or in the hospitals or whatever."

Admin 2 stated that different physicians have different level of access:

> "So certain providers have different access to different parts of the database."

From a privacy professional point of view, a patient consent has to be obtained if the access is out of the circle of care.

PP1 said:

> "Anybody could ask for access, but it is the patients' PI, so they would have to extend of the circumstance of the patient consent (written informed consents) for them to access it or if they are part of the circle of care."

Example scenario to explain the difference between accessing with permission (patient's written consent) and without consent is

> "Let's say that you are visiting the IWK [hospital] and you are having a miscarriage and nurses need to talk to the anesthesiologist they do not need to get your signature or your consent for that circle of care. However, if a researcher doing research in miscarriages has to apply for access to your records without them being anonymized, would need your consent or would have to look at the consent or would have to sign a research agreement of all the confidentiality and so it is not easy for them to bring access to that. It is usually the intent for a researcher is to get anonymized or minimal

> personal information and only if it is required for the research and it is usually done in the double-blind so it is not possible to going and matching back."

Admin 3 is quite strict with only allowing the patient him/her self to access even in the case of spouses. It is a different case when they have a dependent. Parents can access their child information.

Privacy Professional 2 has a different point of view in regard to current practice with most of the information in paper forms/documents:

> "As a current practice, almost everybody can access the records. Let's say that I am newly hired from the quality department, and I need to look at a file and gave them your name, and I wouldn't expect a whole lot of problem in getting your information if they are paper records. If they are in papers, they could be in many places. If they are electronic, I obviously I do not have access to that system. But anybody with access to that system, could probably open your record without much problem and maybe flagged it and audited. Maybe! But unlikely unless their last name matches yours."

IT specialists added to the list of bodies who can access to include physicians, surgeons, and MSI for billing purposes as IT 2 stated:

> "Physicians and surgeons would have that opportunity to access it and they do.
>
> The college of surgeons and physicians is the governing body for all physicians in the province and they will do audit of a physician records. So they used to have paper charts and go over them but now they access to the electronic charts. MSI would also have access and this is not unfired access they cannot just log on whenever they wanted. It would be coordinated by between the physician and other MSI members. So they have to give them permission before they can access. And there would be some restrictions because you cannot just go in and see whatever you wanted. There would be certain records that they want to see and would have to be disclosed to them by the physician."

All participants from the three groups stated that they had assigned unique usernames and passwords and their entire activity is auditable which the IT 2 supports.

Therefore, we know the list of bodies who can access the patients' PHI; what could get access in case the PHI is in paper or electronic format, and we can conclude that are some situations a written consent from the patient is not needed when the access is from the circle of care. Privacy Professional 2 commented on the circle of care regarding privacy and said:

> "Privacy never intended to be a barrier of care."

Patient Access:

For patients to access their own PHI, they need to submit a paper form requesting the access. In larger settings, they need to go to the health record department and ask for the release of the information. In smaller settings, they have to ask the physicians to access (see, make a copy) of their records. If they want to review test results, they have to go to visit the physician. They do not share results over the phone or other ways such as faxes, emails with patients. Otherwise, they notify patients that they need to see them to review tests results.

In the context of having the patient portal, admins set patients accounts through the online portals and then they can access all the information they have about them including test results. Admin 3 said:

> "We have Personal Health Records (PHR). It is called MyHealthNS now. We just set them up with the MyHeathNS, and they would get access their tests results that would be uploaded. It is also used for booking and canceling appointments with me. If I get any upcoming specialist appointments, I can contact the patients through that. It is now the patient's responsibility because it is in the email and password."

If patients' PHI is electronic in the EMRs but that EMR is not connected to the patient portal, patients cannot get access unless they request a copy and pay for printing or downloading in discs (Compact Disc or CD). Admin 4 stated:

> "No way you can go to look at your information in the computer or the system." She commented, "I think that MyHealthNS is all about."

IT 2 stated that the only way patients can access their PHI is through getting printed copies or through MyHealthNS, the patient portal. Privacy Professional supported IT 2 by going first to the caregiver and then if the file is not there, they will refer the patient to where the information is stored.

Therefore, patients must go to the caregiver to be able to get access to their information or log in to the patient portal if the family physician is in the system. They can have both printed copies and digital data. However, they would have to make many trips to be able to get a complete medical file. The information is stored in many places, and systems do not talk to each other (not connected to each other). Even in one system, some departments are not connected as Privacy Professional 2 commented. It is challenging for a patient to have access to their entire PHI.

Limiting Access:

Patients can request not share information, but there is no full guarantee that patient information could be blocked. Admin 4 gave an example from their own experience:

> "We had a situation where my family member goes to the doctor that I am working with and my family member was trying to get pregnant. She does not want me to know and asked the doctor not to let me know. So they could not put it in the record. There is no way you could block somebody from knowing something about you actually."

I believe it is a very critical situation if it is the only way I can block information is not including them in the records, so what happens in the emergency situations or when I need a proof of the condition. It is not the best solution for limiting access.

From Privacy Professional 1 point of view, it is possible to place a note in the file to not disclose the information, and from a computer perspective, you can put locks on. However, Privacy Professional 2 has a different point of view:

> "In technically mature environment where the system has been designed from a privacy perspective, it is even would be difficult, I would say. Ours certainly has not been. We started with Meditech when 2005. Privacy is not the fore front of the system designers."

From IT 2 point of view:

> "We know that NSPHIA gives patients the right to block some aspects of their charts from everyone but the physician. I am not sure how is that going to affect auditing but yes they can do that and through NSPHIA they have that right."

Therefore, it is one of the patients' rights under NSPHIA to limit access to their information. We asked admins, ITs, and privacy professionals if they can do that in current practices. What we concluded is that it is not guaranteed. The patient can have extra notes in their files, but in current practice, there is no guarantee that they can limit who access the information.

Patients can access all information about them as long as the information in their records.

Privacy Professional 2 added:

> "They are expected to get access to whatever information they want if it is available"

Privacy Professional 1 said that it is the right of patients to have access to their records in whatever form of information paper or digital and even if the caregiver ask the patient to pay fess unless:

> "There is something in the file that the administrator or the doctor may feel that (or the clinician, I guess) the delivery of that to you may cause you to hurt yourself or somebody else, very specific and very minimal. It is there especially in case of psychiatric patients."

Therefore, the patient can access any type of information if the information is personally about them in their records. There are some exceptions and are rare and minimal. There is what is called shadow files and notes for doctors that sometimes are not scanned and uploaded into the system. The PP1 said that anything about a patient, the patient has the right to access on whatever form.

Unauthorized Access:

We asked Privacy Professionals about what we could consider as unauthorized access to the information and they both stated: if the information is subject to unauthorized access, stolen, used for undefined purposes, copied, deleted, manipulated is considered as unauthorized access. We asked admins about the current practices when having unauthorized access. Admin 1 said: "Well I will talk to the physician." The admin does not know what next steps he/she has to go through in the case of finding out that there is unauthorized access. Then, we asked if the patient was notified. Admin 1 said that:

> "Patients no. There was a situation that another service faxed over a document that was not a patient of his. We called them back and let them know that hey this document for this person came through but not our patient. They took his details down, and we shredded the documents because it was not ours. I do not know if the

> physician took the extra steps, but I did not. All he did was calling them back to let them know that they are not my patients'."

Admin 3 has a different point of view and their practice is totally electronic said:

> "I would make sure that patient knows and the patient that indirectly involved. And defiantly I would have to notify the patient because they need to know that somebody else's got to read even if it just a fact about them or simple little letters or a referral for a message. It does not matter what it is. It is medical information. So I do need to contact the patients."

In case of patients get access to different PHI of other patients. Admin 4 said:

> "That does happen. So what we can do is just delete it out of there and rescan it to the right record."

In case of receiving information for other patients who are not seen by the physician through fax, admin 1, 2, 3 and 4 said that there is usually a phone number on the cover letter and they would call them back and shred the received documents.

Therefore, we can have admin 1 example of non-compliance case because they did not notify the patient even though the admin knew it is unauthorized access. A compliance example is what Admin 3 did by informing the patient and taking extra steps to recover. I believe it might refer to the years of experience of admin 1, as it is only two years.

Authorized Access:

We asked privacy professionals regarding who give the authorization and allow their access to be authorized access. Privacy Professional 1 said:

> "Anyone who is in the circle of care. They have the right to access without patient's consent and considered as authorized access"

The public Body, which is the Department of Health and Wellness, is the one who assigns the authorization, and everyone in the circle of care has to sign consent form to comply with the PHI confidentiality agreement.

Researchers' Access:

Only 2 admins commented on the ability of researchers to access patients PHI.

Admin 2 said:

> "The patient will have to fill out a consent form especially if we know that we are doing some research in the future, then it would kind of compile all of that information ahead of time, and then they would be contacted."

Admin 3 said:

> "No. They tried to get stuff from the doctor and [she/he] refuses."

Therefore, we had both perspectives. We can conclude that if the doctor refuses, then nobody can access the PHI of their patients. In larger settings, patients have to sign a consent to allow researchers access their information and it is done only once at the registration or opening a file, and then researchers can use the information in future without getting consent.

However, IT 2 who is an EMR advisor said that it is only applied to anonymous data including no identifiers and no need for consent because they have excluded all the identifying information.

5.5.1.2 Personal Health Information and Medical Documents

The code category and sub-codes are shown in Figure 37 in Appendix B.

Either in paper charts or electronic medical files, admins access and retrieve patients' PHI by their healthcare numbers and sometimes by name. There are different types of PHI according to the type of practice and what they are using to manage patients' PHI. For example, Admin 2 only keeps necessary information such as contact information, booking, and registration information on the system while the rest of the PHI is stored in the form of paper charts. Admin 3 keeps everything on the EMR patient account. Starting from contact information, healthcare information, blood work, medical examinations, imaging and referral. We covered the codes of patients' access in the previous *Access* category.

Regarding hosting the PHI, it is either as paper charts in cabinets within the clinic or in servers of the EMRs hosting company. For Practimax, it is a local company, and the server is installed in the clinic. For Nightingale, it is stored outside of Nova Scotia (in Ontario) and the access is remote access to servers outside NS.

Privacy Professional PP1 commented

> "They have to be stored here is NS or in Canada, under Personal Information International Disclosure Protection Act (PIIDPA) unless there is a special

> consideration and given permission of the head of the public body and would be the head minister of the Health Authority or the Health and Wellness Department."

IT 2 commented:

> "It is basically the health information services for the Department of Health and Wellness, and the server is in Young Street as the main server, and there is a backup server off-site somewhere else. All information in servers are stored here is NS because of NSPHIA and other privacy Legislation that no PHI is stored outside Canada for EMRs."

Therefore, we can conclude that the systems and the PHI are under the control of the Department of Health and Wellness, which covers the custodians' responsibilities under NSPHIA.

5.5.1.3 Online Patient Portals

The code category and sub codes are shown in Figure 38 in Appendix B.

For online patient portals, we used MyHealthNs as an example from the current practice. We received three different responses. First, Admin 1 and 2 did not know that there is a provincial patient's portal or PHR, which is interesting. As a provincial project, we can see a lack of awareness of an emerging technology. Second, Admin 4 stated that they are not connected to MyHealthNs and:

> "We looked into that, and we haven't really gone that road yet. The doctors are still not sure what do they think about it. They think it is going to be more work and because they are going to have put the test results into two places, in our system, and to MyHealth."

Admin 4 commented that the healthcare provider that they are working with is going to wait to see what everyone else is using so they can connect them somehow. They work in a small town, and they cover for each other shifts, and they want to connect these EMRs and want to get access to others.

Third, Admin 3 is working in a clinic that has an EMR connected to MyHealthNS. The number of patients who are connected to the EMR through the portal is 800 out of 1400 patients. We discussed the challenges they face in Challenges Section 5.5.1.6. Privacy professional PP2 commented that

> "It is great to use such a technology. MyHealthNS is really great."

IT 1, who is an EMR advisor, stated that all three EMRs have interfaces that could connect to MyHealthNS to facilitate more comfortable managing of PHI and faster access. Therefore, despite the type of EMR used, it can connect to the patient portal in current practice. There are a few numbers of family physicians are connected to MyHealthNS and taking the advantage of the feature as IT 2 stated.

The challenge in current practice is how to get data in and force people to get data in when some family physicians still use paper charts and do not have EMRs. I reviewed the features of MyHealthNS as an online portal. The system is not tested for its usability yet, which may affect patients' experience. How patients access the PHI is discussed in Access Section 5.5.1.1

5.5.1.4 Privacy Compliance and Breaches

The code category and sub-codes are shown in Figure 40 in Appendix B.

We are interested in learning how they comply with current practices and what the privacy professional expects them to do. We asked questions regarding current practices in complying with NSPHIA, and we got different answers.

PP 1 stated that the privacy legislation compliance is higher in Alberta than in Nova Scotia. Risk Impact Assessment is mandatory.

We found that there is not a compliance check for both practices, in paper and in electronic format. PP2 said:

> "There is not a review until there is a compliant submitted."

It is on patients' responsibility to express a privacy concern to the physician to get a response as PP 2 commented. The last thing a family physician want is patient filing privacy compliant to the privacy commissioner. PP 2 said in technological setting, it is a fast number of transactions that could be carried. EMRs have a capacity of auditing that the system cannot exceed.

Preserving the privacy in complicated context such as healthcare systems and EHRs is difficult as PP 1 stated:

> "EHRs sounds great but it is so rainbows and unicorns. Because it has to be done right and it is not easy to do like people would think it is."

Admin 3 said that patients' privacy is maintained in their practice because it is totally electronic. Because of prior experience in a paper format practice, Privacy is not fully maintained.

Measures are taken into account to ensure NSPHIA compliance such as servers inside the clinics located in locked cabinets if they are using EMRs. In a paper format practice Admin 4 said:

> "We had some measure is place like no body can come behind the counter and the charts were back there and the storage room is always locked. We had to use the key all the time to unlock it."

User names and passwords for each employee in the office while using EMRs.

IT 2 commented that there should be reasons to access patients PHI. If you are an admin and have been given a user name and password that means that you can access patients' PHI. Privacy Professional 1 said:

> "In online systems, insuring the person requesting the information has the right of access."

Admin 3 confirmed that they do not share patients' records with third parties nor other physicians.

We can conclude that a full privacy/compliance is not maintained in current practice. It is a better case in clinics using EMRs where the PHI is electronic because the EMRs are already meeting NSPHIA rules and other privacy legislation and placing security measures is mandatory by the law.

In case of the right of being notified when there is a breach is discussed as following:

One of the patients' rights under NSPHIA is to notify patients if their PHI was subjected to authorized access or breaches. We wanted to understand what are the current practices in informing patients and for what cases. We had different answers that revealed a lack of knowledge of patient privacy rights. For example, one of the Admins had a case where PHI of a patient was disclosed to another patient but did not notify the patient and only notified the physician and does not know what the physician did to rectify the error. Not notifying the patient will prevent them from taking the next steps to recover nor practicing their privacy rights. We believe it is due to not having direct contact with patients and their PHI in this case. Such lack of communication can lead to poor management of PHI.

A different situation revealed that doctor office admin knows that notification was patients' rights when an individual called to ask for a copy of another patient One[10] admin said:

> "I notified the patient".

A second admin confirmed that after confirming a breach, they start filling the paper forms of NSPHIA to file the case to the Privacy Commissioner. The current practice reserves a level of privacy but still not in an online way due to the current practices of paper charts.

However, there are not any online notifications yet in current practices because either they are not connected to the patient portal, or they are connected, but they are in read-only status. The notification itself is not very practical in current practices because everything is done in paper or printed formed.

From IT 2's point of view:

> "We know that NSPHIA gives patients the right to block some aspects of their charts from everyone but the physician. I am not sure how is that going to affect auditing but yes they can do that and through NSPHIA they have that right."

Therefore, it is one of the patients' rights under NSPHIA to limit access to their information. We asked admins, ITs, and privacy professionals if they can do that in current practices. What we concluded is that it is not guaranteed. The patient can have notes in their files, but in current practice, there is no guarantee that they can limit who access the information as one right of NSPHIA. Applying the notification feature and situations that notification should be sent to the patient is critical if the online portal show compliance with privacy legislation. We discussed the unauthorized access in *Access* Section 5.5.1.1.

5.5.1.5 Administrators and EMRs

The code category and sub-codes are shown in Figure 39 in Appendix B.

Doctor office admins have set of tasks when dealing with patient PHI. We found that they access PHI and retrieve, create and update the patient medical document, and make appointments. There are different methods that office admins follow to access the patient medical document and different ways to record the PHI.

We found that doctor office admins have a different level of access when dealing with patient PHI. If they are using EMRs such as the case with all four admins, each office admin has

[10] For increased confidentiality, the study participants are not identified, even by number, in this Section.

a unique username and password. The approved EMRs are designed to keep track of who accessed and time/date stamped within the activity record. In case of PHI or medical documents were in paper forms, office admins can get access to the information within the document without being tracked.

Admin 2 who is considering both paper forms and EMR. What they do as admins is retrieving lab results. Admin 1 needs permission every time she/he gets access to retrieve lab results. This permission is gain by conforming username and password for auditing because retrieving is done by connecting the EMR to another system for test results. Admin 1 said:

"What can I access is very limited."

The type of practice where both Admin 1 and 2 that they are considering both paper and system they scan paper charts written by the physician and upload it to the system. Therefore, it is not 100% electronic information. They are electronic scanned files. Admin 2 said:

"That all is ours"

Admin 3 can access, retrieve, copy download any type of information about the patient and make referrals to specialists through the system. The physician is only typing in the visit information.

Admin 4 has limited access as well by only setting up the new account for new patients with new IDs and pull up the account to be ready for the physician. The physician who retrieves all the information he/she needs form the EMR. Admin 4 is working in a practice that is transitioning. They have had paper charts before 2011 and using the EMR since then. Admin 4 commented on why they keep paper charts:

> "We have to keep charts for a certain number of years for ten years especially children. We only can give them a copy we cannot just delete them here we give them the charts in case of moving papers to see a different doctor. And for kids, it is 10 years after they turn 18. So those records "paper records" we are keeping for 20 years. It is crazy and the amount of space. We have both paper and electronically.
>
> The doctors have been in practice for 7 years and we are in electronic practice since 2011. (6 years we have doing it). We did not scan everything in because of the huge amount of work and charts and patients they have. We kind of started at that point. We started from Day 1 kind of thing and went from there. We scan a thing in if it is

> something they refer to and we would have to go back and see it and get it out. If it is something like X-Ray they had 10 years ago and compare it to a recent one. We scanned all the kids because we are going to keep them for a long time. It would be much easier to have it electronically. If we are going to scan everything it would be hiring another person JUST to do that which is overwhelming and time consuming."

We found that admins face some challenges regarding the EMR system that they are using or in current practice and tasks which is included in the challenges section.

5.5.1.6 Challenges and Recommendations

The code category and sub-codes are shown in Figure 41 in Appendix B.

Access Challenges:

Admin 3 stated that they are connected to the MyHealthNS as an online portal and have received complaints that patients are facing challenges in accessing their information especially, the older generation. It might be that the system still developing and new which need some refinements after a while from launching.

At the time the interviews were conducted (2017), the access to the main page of MyHealthNS was difficult. The homepage title was the company name 'RelayHealth' and reaching the main page was through an announcement in local general hospitals to the company homepage and then the portal homepage. IT 1 stated that tried to access it when first heard about it and lost the direction through many steps and did not get the chance to get into it again. Now, they managed a homepage that clearly states MyHealthNS with a direct link. We can relate to the low level of adoption to challenges patients can face to get to the main page.

Privacy Professional PP2 stated that a patient in Nova Scotia has many medical documents distributed throughout hospitals and clinics. To get a complete access, a patient has to make many trips because their PHI is stored in many places and systems do not talk to each other. Even in one system, there are departments that are not connected as Privacy Professional 2 commented. It is challenging for patients to have access to all their PHI.

In emergency situations for ER in hospitals, if the PHI or medical documents of patients not already in the health record of the HER system, there is no way that ER doctors can access the information. We are interested in reasons and asked the Admins. Admin 1 said that ER in hospitals could not access the patients' information directly because:

> “Because it is entirely paper”.

Admin 3 commented that if what they need such as blood work or imaging, they are going to be already in medical records of the hospital systems. Admin 4 said:

> “Quite often they will have ER doctor to call the family physician. So, systems cannot talk to each other. Our doctor can look up the documents from the hospital but the hospitals cannot.”

Therefore, the challenges to access the information is due to how the systems are distributed and not connected to each other besides that some practices still use paper charts which makes not all PHI available online and through systems.

Administration Challenges:

Regarding appointments, Admin 3 said:

> “Some doctors whether their tests good or bad they call you in for appointment. My husband has lost work because he has some health issues right know but he lost work over I got to see a doctor because he called me in to find out that everything is fine”.

We believe that having a PHR or patient portal is going to help and save effort and time. From an administration point of view, Admin 1 suggest that managing online charts is better and more efficient regarding organizing the charts and the medical documents. Admins need education on both patient privacy and how to comply with NSPHIA, especially in current practices where we have different settings as discussed in the Thematic Analysis Section 5.5.2.

Lack of Education Challenge:

We believe that admins need more education on privacy rights for patients and NSPHIA, in general, to show compliance, especially where practices are done in paper forms. To overcome challenges and improve current practices, the privacy Professional PP1 stated that there is a need for doctors’ office admins, family physicians, and everyone in the circle of care to:

- Educate themselves
- Have a good record management system
- Being accountable
- Only collect PI that they required
- Only collect it for the purpose and use it for the purpose

- To hold it securely in confidence, (security protocol whether it is lock in cabined or encrypted)
- Disclose it for the purpose
- How long they are going keep it
- How securely they are going do it.
- How they are going to be destroyed once they are not needed

5.5.2 Thematic Analysis According to the Type of Practice

We analyzed the results according to the type of practice and medium being used to manage patients' PHIs. The results in this section revealed that managing PHIs varies according to the type of practice which would help researchers in understanding the current practices in the province and shed the light on future research studies to draw a complete picture of the current practices. Future research insights are discussed in Section 5.5.3.

5.5.2.1 Electronic and Paper

Admin 1 and 2 consider using both electronic and paper documents. Admin 1 is using Practimax and e-Medical EMR systems. Admin 2 is using MEDITECH along with paper charts. They scan paper charts written by the physician and upload it to the system. Therefore, it is not 100% electronic information. They are electronic scanned files. Admin 2 said:

> "That all is ours."

Admin 1 explained that workers in their office need permission every time to retrieve lab results. This permission is gain by conforming username and password for auditing. The main task is to retrieve a medical document or lab results for the physician. The paper charts are stored in cabinets behind the registration clerks. Mapping to NSPHIA, they need to have physical security measures such as a locked room that only authorized staff can access. Therefore, it is difficult to show complete compliance with privacy legislation in practices that are still using paper charts. Controlling who can access these files is impossible. The solution is transferring to electronic-based systems (EMRs).

5.5.2.2 Only Electronic

Admin 3 is working in a clinic that is totally electronic. They do not have any paper charts. Admin's main tasks include entering patients' basic information, creating a medical document with the system where Practimax is the EMR, retrieving lab results and making referrals. The

EMR is connected to the MyHealthNS patient portal and set up by the admin through the patient's email. However, what patients can see on the online portal is read-only. The physician inserts the visit medical examination and information. Admin 3 can access, retrieve, copy download any type of information about the patient and make referrals to specialists through the system. The physician is only typing in the visit information. Therefore, we can conclude that in practices that are totally electronic are showing compliance with NSPHIA by covering the custodians' responsibilities but improvements to the online patient portal to cover patients' privacy rights under NSPHIA are required.

5.5.2.3 Transitioning

Admin 4 has limited access as well by only setting up the new account for new patients with new IDs and opens the account to be ready for the physician. The physician who retrieves all the information he/she needs form the EMR. Admin 4 is working in a practice that is transitioning. They have had paper charts before 2011 and using the EMR since then. They are using the Nightingale system and not connected to the online patient portal. They are covering the custodians' responsibilities but not the patients' rights.

5.5.3 Mapping to NSPHIA

There are many points that I think we should reflect on what these admins say and what the actual documentation of NSPHIA says. This point will help us outline the difficulties causing this gap. It is out of scope point but to help in bridging this gap; we need to define the reasons behind the gap and the difficulties in applying NSPHIA in current practices.

For the question: what are the types of PHI that they process and what we consider as PHI, we got different answers. For example,

Admin 1 says:

> "All patient contact information, which include: name, address, healthcare information, blood work and imaging."

When we link what they think PHI is and what they know, we can see that the definition is more than that. This point leads to the awareness they need to receive as admins when dealing with sensitive information of this kind.

Admin 4 says in the case of confirming that there is breach and filling out the paper work of NSPHIA that is:

> "It is a lot of paper work".

It is patient's rights to limit who can access their information. But in current practice it is not guaranteed "it is impossible" what we can offer in this situation is what we plan to do. From privacy professional's 1 point of view in the ideal situation:

> "The information is the information. The information, is the record, is Personal Information whether it is in paper format or electronic format. The same access rights and privacy rights apply to that information."

We found that there is a lack of awareness on the next of steps that should be taken into account in case there is identified breach. Admin 1 said that they would never inform the patients and leave it to the physician to decide what should they do.

One important point is that while I was distributing the recruitment notice, I notice that in the case of having paper medical documents, they were in open cabinets behind the admins without any physical locks. This shows a failure of compliance to the PHI in NSPHIA such as in the cases of Admins 1 and 2. Admin 3 commented on this from her experience working in offices that are totally paper-based:

> "I had worked in an office who would hang all the documents that they need to see tomorrow and cleaners would come in some offices here. There is nothing in locked door or looked cage. Anybody goes into that office can open or pull any chart."

The lack of review by NSPHIA is discussed in the following section.

5.5.4 Suggestions to NSPHIA from a Technological Perspective

Based on the analysis of NSPHIA and the current practices, we suggest some aspects as follows: First, we learned that there is not a sort of compliance check performed by the department of health and wellness and NSPHIA. We raise some questions:

- Why there is not a periodic compliance check?
- How do they know that clinics follow the rules of NSPHIA?

However, they only start to investigate when there is a complaint.

Second, NSPHIA gives everyone in the circle of care the privilege to access Patients' PHI, but they did not specify who is in the list of the circle of care. We commented on this point because of the clinic that is transitioning, which is used to have paper charts and now uses EMR system. Three family physicians, two administrators, a receptionist and a practice nurse and an office manager are all have access to patients' records. Therefore, we need to know:

- A defined list of members of the circle of care.

This point leads to a new idea, which is:

- Why there is not a defined level of access (certain privilege) to different types of PHI and should all members of the circle of care have the same level of access?

5.5.5 Research Insights to Expand the Study

The results of the study revealed research areas that we still need to learn to draw a complete picture of the current practices in the management of the PHI in Nova Scotia, which we suggest, to researchers as future research areas to expand the study to cover the following research questions:

- Why still doctors do not use the recommended EMRs? Is it the price? The number of patients? The doctor level of technology proficiency? Rural or urban area? The lack of education on the advantages? What are the real reasons behind not using the EMRs?
- What are the reasons for using paper charts while every practice can be digitalized and have approved three EMRs?
- Why some family physicians who are using EMRs still not connecting to the online patient portal?
- Why still patients have multiple versions of their PHI distributed over different systems in NS (SHARE, MyHealthNS, EMR, and EHR)?
- Why there is not a unified record? What are the reasons for impending this from happening?
- Why still parts of EHRs are not talking to each other (not connected) even in one setting (hospital) what technological and legal perspectives should be covered to make it possible?

5.5.6 Study Validation

Charmaz (2006; 2014) identified evaluation criteria used when the grounded theory is applied, which include: credibility, originality, resonance, and usefulness.

5.5.6.1 Credibility

Credibility refers to the strong connection between the gathered data and the study argument and research questions, and if the study provided the richness of data and expected quality (Charmaz, 2014). I believe that the emerging framework covered the aspects that are needed to understand the current practices and propose the design guidelines to be used for the next research phase.

Second, we have used more than one source of information to form the interview questions; the questions were refined after piloting the interview and reviewed by the supervisors. The self-training I received to conduct the in-depth interviews helped in obtaining rich data that are relevant to the both PHIA as an emerging law and the management of PHI in current practices.

To enhance the analysis process to form the framework, the in-depth interviews that have probes emerged from the discussion afford the study with precious data. I, as the principal investigator and interviewer, conducted the interviews due to the hybridity of the context starting from the NSPHIA analysis and the proposed privacy patterns along with background information to provide appropriate probing questions. Also, during the analysis, using memos with the reflection after each interview helped in mapping the data and provide categories that most relevant and most important to consider.

5.5.6.2 Originality

Originality refers to the state of proposing new insights and contributions (Charmaz, 2014). I believe that the framework proposed form the study shed the lights on new insights regarding the integration of privacy law requirements as design requirements. The study not only proposes the framework as design guidelines but also explains the current practices for designers. This would help designers to cover aspect that they might not think off due to the complexity of the context.

The study supports the concept of expanding the concept of end-users to include anyone who is privacy law user and using eHealth to ensure compliance and manage patients PHI. Using privacy laws as a departure point was a first in which the literature lacks reference to legal frameworks from the IT perspective. Using the grounded theory as an analytical tool to propose design requirements is emerging, and we try to support it.

5.5.6.3 Resonance

Resonance refers to how the categories are rich to describe the study research objectives and how the analysis offers profound insights. The developed framework consists of categories that were generated from the interviews that cover the basic themes emerged from the Thematizing stage of the study. The connection between the categories and the details provided in analysis process are rich. Each category including sub-codes was identified and explained through the data analysis, and the interviews underwent several reviews as well as a recoding, and comparing the data to achieve a clear identification and explanation of the properties of each concept. I also added in regular consultations with my thesis supervisor and another committee member to discuss the research process at important decision points.

5.5.6.4 Usefulness

In brief, the results of the study should be applied in the field of Information Technology in the context of eHealth to provide both privacy compliance and privacy-preserving designs guidelines. The framework was tested for validity in the next Phase in which the richness of the input resources and the feedback from the different stakeholders were examined to address privacy from a legal perspective and for privacy professionals to support IT designers.

5.5.7 Limitations

The study was subjected to several limitations as follows:

First, we found that there are different types of clinic settings including only electronic, using both paper and EMRs and transitioning who used to use paper charts and now are using EMRs. We had the chance to cover all of them. However, we need to cover the only paper type of practice. Further research is needed to draw differences between current practices.

Second, the study has limited number of participants for several reasons discussed in the sampling section (5.1.4). However, “a small number of interviewees is enough unlike other quantitative research methods such as surveys when a generalization is needed” (Guion et al., 2001). The original plan was to cover the legal perspective by interviewing who designed NSPHIA as NSPHIA representatives; however, the lack of interests was a barrier. We then thought of local privacy professionals as a source of information as they have experience in both, health information/systems and privacy legislation. Recruiting different participants’ groups would add to the general understanding of the study such as IT staff from larger contexts in hospitals, NSPHIA representatives, and privacy lawyers to add to the legal perspective covered in the study.

Third, to understand current practices we had to limit the context to the setting in Figure 3. Covering larger context such as EHRs systems in hospitals and how they comply with NSPHIA would add more categories and shed the lights on understanding the flow of the PHI between system sections and online portals. Fourth, our case with NSPHIA as a new legislation and the patient portals was launched last year is not the ideal. However, we believe understanding the current practices will help IT designers adopt what they fit their contexts in applying the design guidelines. Applying the framework in already working patient portal might reveal aspects that are not covered in this study.

5.5.8 Potential Contributions

Based on the results, we propose privacy-preserving design guidelines that were used to form the tasks as an output from the study and input to the following cooperative prototyping sessions; and general design guidelines that would help designers in the analysis and design phase of eHealth Applications based on our study results.

5.5.8.1 Privacy–Preserving Design Guidelines

1. **Notice/Notification and Data Collection**

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to privacy principle
1	Define PHI collection	When the patients' PHI is collected for defined purposes	P1[11] P4	•Who accessed •When •Patient consent	Collection Limitation
2	Define secondary use of information	The patient's PHI was collected for undefined purposes	P1 P3 P4	•Who accessed •When •Why •Patient consent	Collection Use, Retention and Disclosure limitation

[11] P refers to the Privacy Pattern from previous phase.

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to privacy principle
3	Notification of unauthorized access	The patient either found that his/her information was subjected to unauthorized access	P1 P4	•Who accessed •When •Why	Accountability Breach
4	Notification of unauthorized modification	The patient wants to be notified/informed when there is a detected unauthorized access	P1 P2 P3	•Who, When, What type of information is subjected. •Third parties •Healthcare professional	Accountability Breach
5	Notification when PHI is disclosed	The patient wants to be informed when their PHI is disclosed to be able to review the list and apply restrictions	P4 P3	•Disclosure outside NS •Inside NS	Accountability Use, Retention and Disclosure limitation

Table 7. Notice/notification and data collection design requirements

2. Data Access

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to privacy principle
6	Access PHI	The patient wants to access their personal health information a and review what is collected about them	P1 P2	•How •Authentication techniques that best fit patient's needs •What sources of information EHR, EMR, tests, imaging, etc.	Individual Participation and Access Openness, transparency and notice

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to privacy principle
7	Correct PHI	The patient found that part of their PHI is not correct and they want to correct it	P1 P2	•How •What type of information need to be reviewed by healthcare providers and what does not need to be reviewed	Accuracy and quality Openness, transparency and notice
8	Check PHI is up-to-date	The patient found that their information is not up-to-date and they want to add dome information	P1 P2	•How •What type of PHI that they are allowed to add by themselves •Waiting for the review	Accuracy and quality Openness, transparency and notice
9	Add PHI to the record	The patient wants to add more information to their records	P1	•How they are marked that it is from patients, not healthcare providers	Accuracy and quality Openness, transparency and notice

Table 8. Data access design requirements

3. **Information Disclosure**

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to Privacy principle
10	Set a pre-defined list of providers and custodians	The patient is interested in specifying a pre-defined list in which a certain number of healthcare	P3 P2	•How •What consequences they need to know before applying this feature •When they can	Consent and Choice Purpose Legitimacy and Specification Activity record

No.	Privacy requirement	Task Scenario	Privacy pattern	Notes during prototype	Mapping to Privacy principle
		providers and agents can access their information or collect them.		and when they cannot	
11	Limit the list in the activity record	The patient found after reviewing the activity record is that they want to either hid part of the information or want to apply restrictions and limit the list of who can access the information and/or collect them	P3 P4	•How •What consequences they need to know before applying this feature •When they can and when they cannot	Consent and Choice Purpose Legitimacy and Specification Activity record
12	Request to block all	The patient wants to apply a feature of blocking all information.	P3 P2	•A discussion of consequences •When and what type of PHI they can apply the block all.	Consent and Choice Purpose Legitimacy and Specification Activity record

Table 9. Information disclosure design requirements

4. Consent

No.	Privacy Requirement	Task Scenario	Privacy pattern	Condition/Note	Mapping to Privacy Principle
13	Obtaining agreement on custodian privacy policy	Patient wants to review the custodian's privacy policy.	P1 P2 P3 P4	•What type of information •Opting in and out •Time stamp •Negotiation	Consent and Choice

No.	Privacy Requirement	Task Scenario	Privacy pattern	Condition/Note	Mapping to Privacy Principle
14	Obtaining agreement to collect information	Patient wants to know who is collecting their PHR and for what purpose to be able to decide whether to give consent or not.	P1 P2 P3 P4	•What type of information •Opting in and out •Time stamp •Negotiation	Consent and Choice Purpose Legitimacy and Specification
15	Obtaining agreement to third party	The patient wants to opt in and opt out from an agreement with the third party in case their information is outsourced.	P1 P2 P3 P4	•What information •Opting in and out •Time stamp •Negotiation	Consent and Choice

Table 10. Consent design requirements

Our design guidelines are different from other privacy principles such as ISO privacy Framework and other general design guidelines regarding the legal perspective that they are based on. We used NSPHIA in Nova Scotia as a departure point to represent privacy legislation. By applying the guidelines, we believe that the online portal is complying with privacy legislation and maintain a reasonable level of privacy.

5.5.8.2 General Design Guidelines

These general guidelines either we figured that need to be covered by NSPHIA or find out that we need to be covered during the analysis and design of any eHealth technology that is privacy-compliant. These guidelines are based on the analysis of the qualitative data gathered from the interview study and NSPHIA legislation, which is listed as follows:

PHI Access

- Define the authorized and unauthorized access cases
- Identify who can access PHI with and without patient's consent
- Define what they can access? Part or a full record of PHI?
- Identify the types of PHI that can be accessed by different stakeholders
- Identify how different stakeholders get access?
- Identify the purposes of access and time limits?

- Detect where the PHI is stored and who is responsible for hosting the information and in what forms
- What are third parties' responsibilities and their limits of the disclosure

Privacy Legislation and Breaches

- Define what is considered as a breache
- Analyze the case of previous breaches
- Identify steps to recover from both custodian and patient perspectives
- Identify cases were breaches could happen
- Identify privacy measures such as protection techniques and online consent
- Define custodian responsibilities regarding the measures taken to protect the PHI
- Privacy legislation review of compliance

Patients' Access and Online Portals

- Identify cases were patients' notification is mandatory by the privacy legislation
- Design privacy notifications that are meaningful and simple with regards of usability aspects
- What a consent form should include under the privacy legislation and when consents should apply
- Provide patients with the ability to limit who access the PHI, what they can access, and keep activity record.
- Provide patients with ability to access, correct, download and print their online PHI

5.6 Conclusions from Phase Two

We have presented a detailed interview study to understand current practices in managing PHI for both EMRs and online portals. We covered the administration, technological and legal perspectives by interviewing doctor's office administrators, IT specialists, and privacy professionals. We used Grounded Theory as our analysis approach to find the themes we needed to cover in our next research phase. Based on the results, we proposed several privacy-preserving design guidelines to help IT privacy designers show compliance to privacy legislation in the design process of online patient portals in Canada. In future research, we will apply the design guidelines in online patient portal proof-of-concept scenarios. By conducting in-depth interviews with different stakeholders who are NSPHIA users, we could draw a complete picture of current practice regarding privacy legislation compliance. We believe that by applying the in-depth interview approach in this study, our research can have a clearly defined path to follow in designing the cooperative prototyping workshops for online portals that should be usable and privacy-preserving, and that light will be shed on additional research areas for designers who are struggling to understand how different stakeholders manage patients’ PHI.

6 Chapter 6: Phase Three Cooperative Prototyping Sessions

In this chapter, we include the study design of the Cooperative Prototyping Phase. It starts with rounds of the initial sessions as a Collaborative Analysis of Requirement and Design (CARD) approach and productive sessions, during which we apply our proposed Decision-Making workshop as a Participatory Design methodology and a form of cooperative prototyping.

6.1 Related Work

There are numerous approaches through which cooperative prototyping can be conducted. Cooperative prototyping is an iterative process that primarily involves low- and high-fidelity phases (Waart et al., 2015).

Storyboard prototyping shows its importance in helping designers to determine users' needs and requirements from an early stage which provides a basis for further usability testing as next steps (Landay, 2015).

PICTIVE is a form of mock-up that offers pencil concretization of the eventual outlook of the desired technology (Muller, 2015). PICTIVE is of importance in participatory prototyping in several ways. PICTIVE makes it possible for the low-fidelity prototype to be modified by the end-users in the design process in which the modification can take place in real time (Muller, 2015). As a result, it is possible to ensure end-users' satisfaction as well as providing a platform for further creation and enhancement of the interface represented by the mock-up (Muller, 2015).

The most common form of PD is the Future Workshops by (Kenssington and Madsen, 1991; see also Bodker et al., 2004; McPhail et al., 1998; Kensing & Madson, 1992; Morch et al., 2004), in which participants develop a critique of the present situation and envision the future by implementing potential steps from present to future. Another type of cooperative prototyping is the proposed workshop by Buur et al. (2000) where participants develop a mock-up and then act out a video scenario.

An interesting novel PD workshop was proposed by (Druin et al. (2009), who designed the session in a way in which the classroom floor was the design surface. Cooperative Interactive Storyboard Prototyping (CISP) plays a crucial role, as it helps to bridge the divide that exists between developers and end-users (Arnowitz & Arent, 2010). The Software Sharing Workshop approach, in which a virtual workshop where participants from multidisciplinary backgrounds meet online in one session, was proposed by Costabile et al. (2006). Narrative designs are constructed by the designers and examined by the participants for the purpose of exploring the functional design, which are known as science fiction prototypes (Grimshaw & Burgess 2014). The reality workshop was implemented by Weber et al. (2015) to examine the benefits of using PD techniques for enhancing the UI designs.

The CARD by (Tudor et al., 1993; Muller et al., 1997) is an informal, semi-structured technique where different stakeholders participate in collaborative analysis and critique of tasks flows in a system design. We plan to apply the CARD approach in the initial sessions for several reasons discussed in Section 6.3.

6.2 Research Objectives and Questions

The main objective of the study relates to the overall objective of the thesis, which is to bridge the gap between privacy professionals and IT designers by providing privacy designers with a privacy-preserving framework based on Canadian privacy legislation.

A second goal is proposing and exploring co-design methodologies to understand how multidisciplinary participants interact, share experiences and knowledge from different perspectives, and create a common language. A common language would then help form collaboratively agreed-upon designs that are usable and privacy-preserving.

We plan to understand how multidisciplinary participants construct design ideas to create both common understanding and designs. Additionally, we aim to provide a mutual learning process between all stakeholders who are involved in the design process and can influence design decisions. The research methodology is designed to focus on how we integrate privacy law requirements as design requirements.

The research questions to cover the research objectives include:

1. How do different stakeholders, who are considered to be NSPHIA users who should show compliance, understand privacy law requirements and apply them during the prototyping sessions, given their limited law background?
2. How are end results affected by integrating privacy professionals and end-users in cooperative prototyping?

3. How do multidisciplinary teams in cooperative prototyping sessions affect the process of constructing ideas?
4. How does collaborative design research affect the outcome of co-designing by different stakeholders?

The initial hypotheses include:

1. Integrating input from privacy professionals at every stage of the design lifecycle will enhance the level of the privacy
2. Integrating input from different stakeholders along with end-users from the early design phase will increase the level of usability and help in understanding their needs
3. Cooperative designs that involves stakeholders from different backgrounds lead to outcomes that may be substantially better from what purely IT-based designers might design

6.3 Research Plan

Our cooperative prototyping study is divided into three sessions. There is an initial session, which is a CARD technique, and two productive sessions, during which we apply our proposed Decision-Making workshop.

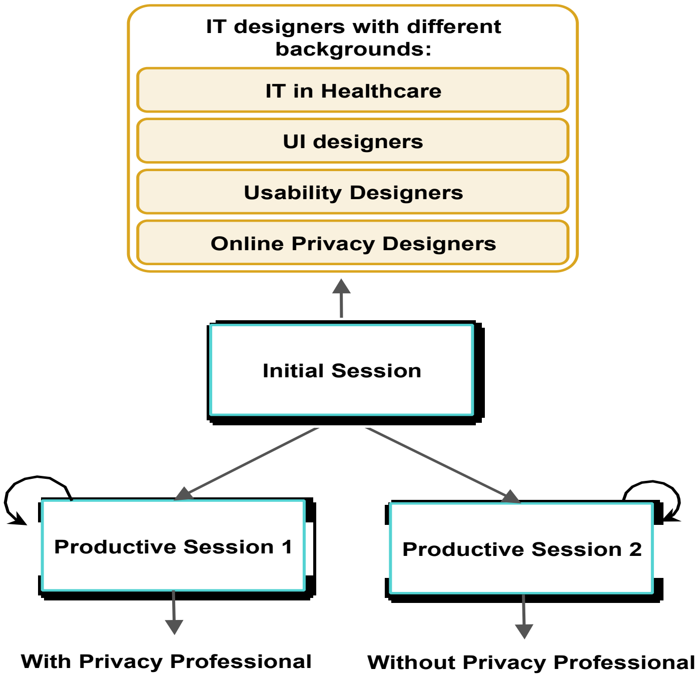


Figure 8. The cooperative prototyping sessions

They were planned to be held separately starting from the initial session and followed by the two productive sessions (as shown in Figure 8) for at least three rounds. The objective of conducting three rounds of the productive session is that we might not get what we need from conducting only one round. Both productive sessions included the same tasks, and, during these sessions, all stakeholders actively influenced the design prototype.

In the following sections, we divided the two parts of the study based on the sessions. Each part includes study design, data collection, analysis, results, and discussion.

6.3.1 Study Participants

We recruited 30 participants: 12 participants for the CARD sessions and 18 for the Decision-Making session. The number of participants is determined according to the literature review to produce the intended results (Muller et al., 1993, 1995, 1996; Macaulay, 1995; Wright & Monk 1991).

For the CARD sessions, we only need IT designers, and, for the DM sessions, we need the multidisciplinary team of the following list. Therefore, the target population includes the following:

- IT designers with different backgrounds ranging from privacy, human factors, usability, and health informatics; are recruited by sending recruitment emails to the mailing list of the Faculty of Computer Science <csgrads@cs.dal.ca> and <csall@cs.dal.ca>
- Privacy professionals, including professors from the School of Information Management and the School of Law at Dalhousie. E-mail messages and the recruitment script are sent to a predefined list of professors who are privacy professionals and/or have privacy as their main research interest and to graduate students <listserv@lists.dal.ca> and <dalsim-grad@lists.dal.ca>
- Individuals from the public who are using online patient portals and/or personal health records or are interested in using them and are at least 17-years and older. They are recruited by placing posters in public places, family physicians' waiting rooms, and around the Dalhousie campus

6.3.2 Data Collection

The collected data are in five forms: audio, videotaped dialogues, notes, artifacts (paper mock-ups of screens), and questionnaires. The principal investigator was taking observational notes during the study, which are augmented with the recordings to enable capturing of more details for analysis purposes.

Data are collected according to the session as follows:

- For the initial session, we have only paper mock-ups of screens, videotaped dialogues, and notes
- For the productive sessions, we have video and audio recordings and notes of discussions on a set of functions derived from the tasks that are defined form the initial session

For each session, we form a summary sheet to capture themes and key aspects. Some qualitative sheets are combined to finalize the key aspects of the design and both demographic questions (pre-session) and the post-study questionnaire at the end of the session (which are shown in Appendix E).

6.3.3 Study Tasks

In Appendix D, the tasks are organized according to categories. Each category includes a list of tasks. I listed all points/questions that need to be covered during the sessions. Each category table includes the number of the task, the privacy principles according to ISO 29100, scenario, the privacy pattern they are mapped to, notes during the design, and the next or following task.

These tasks were analyzed before they used by the CARD sessions and after. Each refinement is mentioned at the beginning of tasks sections.

6.4 Study Part 1: The Initial Sessions as a Collaborative Analysis of Requirement and Design (CARD)

In the initial session, we are going to apply the CARD technique (Tudor et al., 1993; Muller et al., 1997). CARD "is a participatory technique for analyzing task flows and for redesigning task flows, in software systems" (p. 1) (Tudor et al., 1993). It is an informal semi-structured technique where different stakeholders participate in the collaborative analysis, and critique of tasks flows in a system design. It is designed to be applied in the early design cycle, especially at the task analysis phase (Tudor et al., 1993).

6.4.1 Methodology

The objective of this session is to refine our initial requirements and tasks. The initial tasks usually reflect the designer's initial understanding of the early requirements.

The reason behind using the CARD technique is that it helps to analyze, criticize, and redesign the tasks' flow, which prepare the task scenarios for the following session.

Each participant sketches the design element and passes it to the next participant. The design is discussed as a group before moving to the next task. The participants were provided with cards, headers, pop-up windows, icons, highlighters, pens, pencils, and sticky notes.

The list of tasks is based on the proposed privacy-preserving design guidelines from the in-depth interview study supported with the integration of the design solutions from the privacy patterns. The list of tasks reflects our initial understanding of the early requirements along with the input from different stakeholders' feedback from the interview study. The list of tasks is included in Appendix D.

The open discussion on the tasks was expanded to help us get feedback from different points-of-view regarding what can be applied, the possible trade-offs, and ways to overcome issues. Having multidisciplinary teams with different backgrounds and experiences in one session is becoming essential and more common (Dayton, 1991; Muller & Cebulka, 1990).

This discussion can be applied one-on-one or in groups; however, we plan to have small groups of three to five participants to allow a greater level of participation from all participants. We felt that many smaller rounds of discussion with different participants would maximize the participation and the input more than one large number of participants. We planned to have rounds until we reach data saturation.

As a result, we have applied a high-level task flows analysis, and all stakeholders who participate in this session are considered as co-investigators, designers, and co-evaluators of the tasks' flow. The results from the session are analyzed, and reflected and mapped to NSPHIA regulation, which provide a ready list of tasks for the following session as an input, as shown in Figure 9.

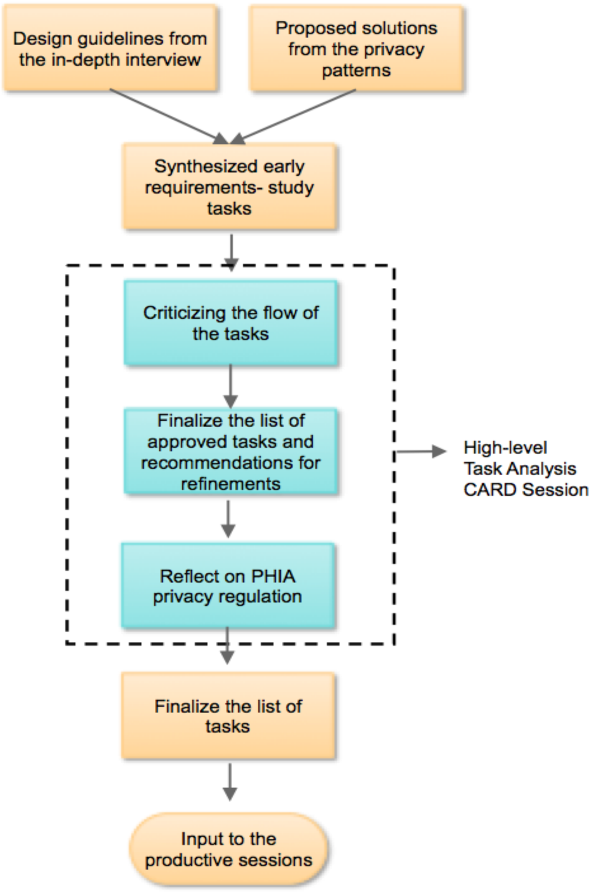

Design guidelines from the in-depth interview
Proposed solutions from the privacy patterns
Synthesized early requirements- study tasks
Criticizing the flow of the tasks
Finalize the list of approved tasks and recommendations for refinements
Reflect on PHIA privacy regulation
High-level Task Analysis CARD Session
Finalize the list of tasks
Input to the productive sessions

Figure 9. The initial session—CARD

One limitation of the methodology is that the IT participants dealt with already existing tasks flows and criticizing them instead of creating their own tasks. We can get their suggestions in the open-ended questionnaire; however, we had to plan the tasks because we want them to be privacy-preserving and based on privacy regulation. Also, for more formal analysis, the results of this session should be supported by other techniques to provide a formal source of information in which we are planning to do the following productive sessions.

The CARD technique can relate to other similar methods and differ. For example, CARD, in some ways, is similar to card-sorting, where participants sort the cards according to the sequences of the task or steps (Neilson, 1993). However, it differs in a way such that participants are considered as a source of information and co-designers. In card-sorting, the results are focused on either similarity or preferences, while CARD generates rich, complex, and related aspects of the discussion. Moreover, in traditional card-sorting, cards are not annotated, and participants only focus on the flow of steps. However, in CARD, each card must represent a task with all its steps.

CARD can relate to the Organizational Kit and Layout Kit participatory design approaches from the literature presented by (Klær & Madsen, 1995). They share the concept of having informal group activities using cards; however, in CARD, the cards represent a task and its following steps to examine the flow of the task, and it is used in combination with reconstructing the tasks and determining if the task or the step should exist.

Our minor contributions to the CARD technique include the input to the session being a result of proposed design solutions based on (1) a legal framework (NSPHIA) and (2) a consequential analysis of early design requirements.

6.4.2 Data Analysis

The analysis process was divided into two parts based on the methodology that we followed: three rounds of CARD sessions followed by four sets of cooperative prototyping sessions—two with privacy professionals and two without.

The data collected in the three rounds of the CARD sessions were analyzed to provide high-level task analysis by preparing the tasks (design guidelines) for the following step of the study. The CARD sessions, as mentioned, are only conducted with IT designers. A total of 12 participants were recruited for this phase distributed as 4 participants in each session.

6.4.3 Participants' Demographic Information

Participants' demographic information is shown in Table 11.

ID	Age	Gender	Education	Experience	Area
1	26	Male	Masters degree	1	Usability
2	35	Male	Doctoral Degree	7	HCI
3	27	Female	Masters degree	4	Health Informatics
4	34	Female	Doctoral Degree	3	Health Informatics
5	31	Male	Doctoral Degree	8	Health Informatics
6	29	Female	Doctoral Degree	5	Mobile Health
7	26	Female	Masters degree	1	Information Technology

ID	Age	Gender	Education	Experience	Area
8	28	Female	Masters degree	1	Data Management
9	25	Male	Bachelor degree	2	Online Privacy
10	49	Female	Post graduate honors' degree in design (B.Des)	1	Privacy and HCI
11	22	Male	Masters degree	1	Security
12	38	Male	Masters degree	5	Machine Learning

Table 11. CARD sessions' participants demographic information

6.4.4 Results

The research outcomes from conducting the three initial or CARD sessions are intended to provide a high level of task analysis for our pre-design requirements. In this section, we organize it as follows: the analysis of the tasks, the preliminary framework, and the post-study questionnaire.

6.4.4.1 Pre-design high level task analysis

We organize the results of the rounds based on the main themes discussed in the sessions. The tasks tables from the previous chapter are used to guide the discussion.

- **Unauthorized Access Notification Task**

We refined the list of tasks that resulted from the previous phase. We have combined Tasks 3, 4, and 5 under Notification of Unauthorized Access.

Task #	Privacy Requirement	Task Scenario	Privacy Pattern	Notes During Prototype	Mapping to Privacy Principle
3	Notification of unauthorized access	The patient either found that his/her information was subjected or accessed to unauthorized access	P1 P4	•Who accessed •When •Why	Accountability Openness, transparency, and notice

Task #	Privacy Requirement	Task Scenario	Privacy Pattern	Notes During Prototype	Mapping to Privacy Principle
4	Notification of unauthorized modification	The patient wants to be notified/informed when there is a detected unauthorized access	P1 P2 P3	•Who, When, What type of information is subjected. •Third parties •Healthcare professional	Accountability Openness, transparency, and notice
5	Notification when PHI is disclosed	The patient wants to be informed when their PHI is disclosed to be able to review the list and apply restrictions	P4 P3	•Disclosure outside NS •Inside NS	Accountability Use, Retention, and Disclosure limitation

Table 12. Notification of unauthorized access task

During the discussion, participants had general ideas that they need to consider more aspects than the ones listed in the table above. First, notifications should not be numerous and overwhelming, and they need to be concise regarding content. Limiting the number of notifications will help end-users manage them without being distracted. Participant ID 1, who is working in HCI and usability testing, said

> "I think there is some information or some information that would be identified that is not necessary, so getting those kind of alerts would be disturbing and it would just raise unnecessary tension. So, there should be restricted amount of notifications."

Before sending notification to end-users, the notification should be classified based on the concept of active and passive alerts. Active warnings "force users to notice the warnings by interrupting them", while a passive warning is a pop-up window that does not interpret the user activity (Egelman et al., 2008) and often fails to draw end-users' attention (Wu et al., 2006).

- **Design requirements**

The idea of using the active and passive warnings was proposed by an HCI Ph.D. candidate, Participant ID 2, who has experience in UI design. It was interesting and gained participants' attention to build on the idea by adding another level of classification—color-coding. Therefore, participants suggested that before sending a notification, it should be classified by both active and passive warnings and color-coded. For unauthorized access, the warning should be active and in red. The end-user must take action, and the window will not disappear until the user clicks on ‘close’. Participants suggested a link to a detailed version of the warning that is listed in the alert tab or Warnings Collection section on the portal. The active warning should be in the middle of the screen where everything else on the online portal is blurred.

Figure 10 illustrates the design ideas resulted from the discussion during the three rounds.
For the passive warning, it should be either medium risk with yellow color or low risk with green color, and the warning will disappear after a while but still be listed in the Alerts tab.

From the first round of discussions, it was decided that the notification design should be in the form of a pop-up window, but the alerts should be classified using the color-coding. Additionally, color-coding should specify the severity of the notification: red for high risk, yellow for medium risk, and green for low risk. A red notification always pops up automatically, while yellow and green show a badge in the Alerts tab or message center. The idea of having an alert tab was suggested in all three sessions. However, three options were suggested in the first round: the presence of only active messages, as suggested by Participant ID 4: “the notification, in general, for unauthorized access should be in the middle and not in the right or left”; only an Alerts tab, as suggested by Participant ID 1; and a red icon beside the username that leads to more details, as Participant ID 3 suggested: “a button on the top right of the portal [the home page] that is either red or green.” Further discussing these three options, participants agreed on two design elements: (1) an active warning that requires action and (2) when it is closed, it takes the end-user to the Alerts tab, where they can manage the warnings according to their severity or risk level.

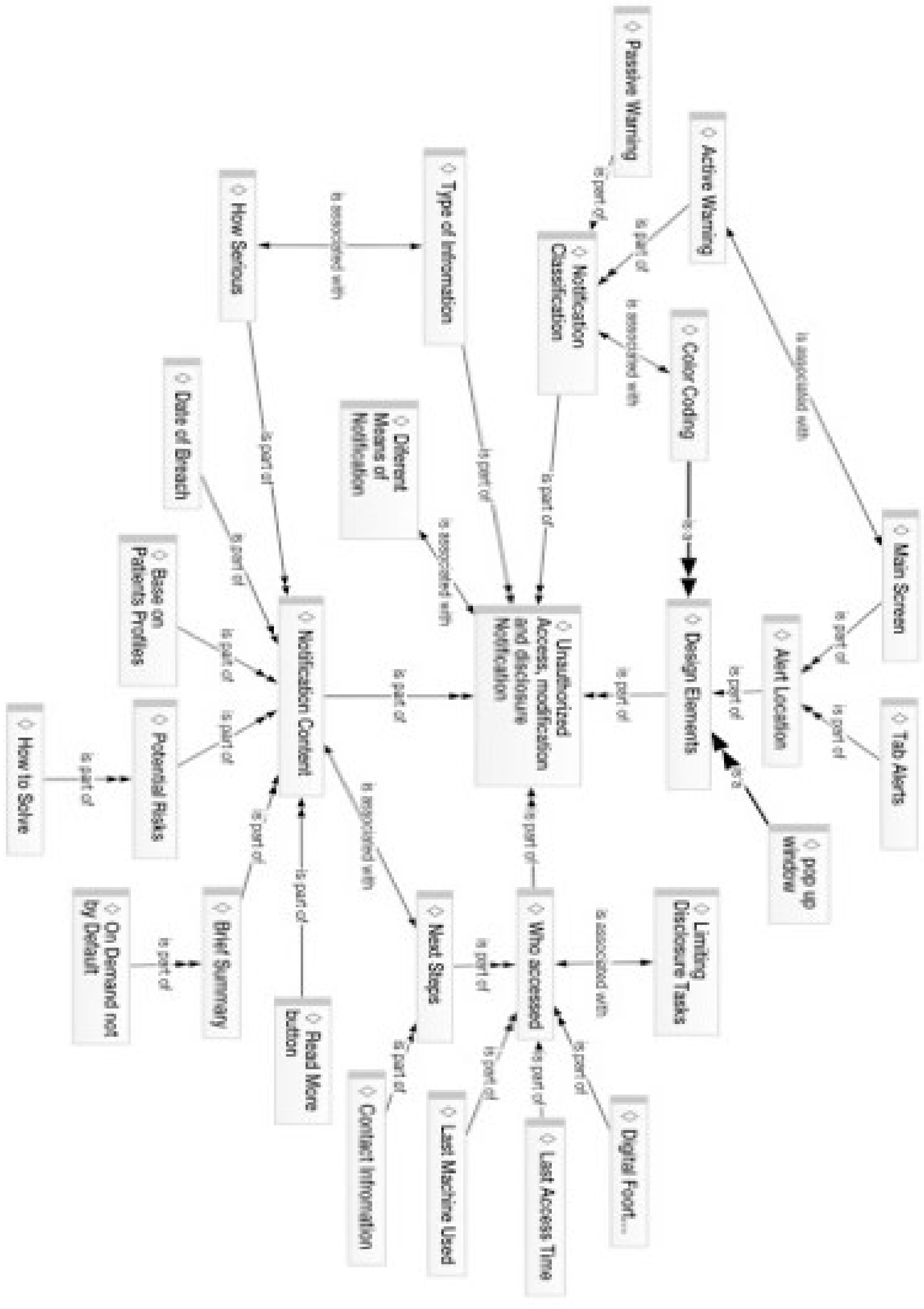


Figure 10. Unauthorized access and disclosure notification aspects

The second and third rounds suggested using the same design elements, including pop-up windows and color-coding. However, the discussion regarding the Alerts tab was the main focus in the second round after dealing with the pop-up notification. Participant ID 6 suggested another idea besides the pop-up window—a red header in the homepage of the online portal and on the login page. In Round 3, Participant ID 10 suggested the idea of a Message Center, which, after the discussion, turned out to be similar to the Alerts tab.

Finally, the notification, in general, for unauthorized access should be in the middle and not in the right or left. Participant ID 1 commented that, "[the best location for the notification is] in the middle or end-users might ignore it [because they may think it] is an ad." A Report Incident button is also important, as suggested by Participant ID 2.

- **Notification content**

From the both first rounds, participants focused on the content of the notification.

  - **A brief summary of the breach**

Participants discussed the ability of not having an overwhelming message—one that starts with a summary and then a link to a full version of the notification. For example, explaining the risks in the notification itself is going to frighten the end-user, as Participant ID 6 mentioned. Participant ID 5 stated, "It is better [for the notification] to be a summary and then on demand [in] my opinion." The participant suggested that the content should focus on what the custodian is doing to recover from the breach to present the information in a way that does not lead to alarming the user.

A different idea, proposed by Participant ID 10 of the third round, was that the message should contain a number to call for more clarification. "They can contact a real person [or] a phone number or an email address to read more information," as explained by Participant ID 10. The idea was suggested to help the end-user have more contact to the details of the breach because the pop-up window will disappear after reading and closing it.

Participant ID 10 suggested having a contact method that would make the end-user take a step forward in understating the breach because the pop-up window will disappear after the clicking on the close window. Participant ID 9 disagreed and mentioned, "It might be frustrating because it is not the fault of the user and it does not seem realistic to call the healthcare custodian for a privacy breach that they were the cause of" and supported the idea of having an acknowledgment type of messages.

However, the other two participants, ID 11 and 12, agreed on having contact numbers as part of the next steps because end-users need to feel that they have a level of control or that they can do something about it.

The summary should include: the title of the alert; IP address of the unauthorized access; suggested actions, as offered by Participant ID 4 from the first round; the date of the breach, as indicated by Participant ID 5 from the second round; and potential risks, as provided by Participant ID 11 from the third round.

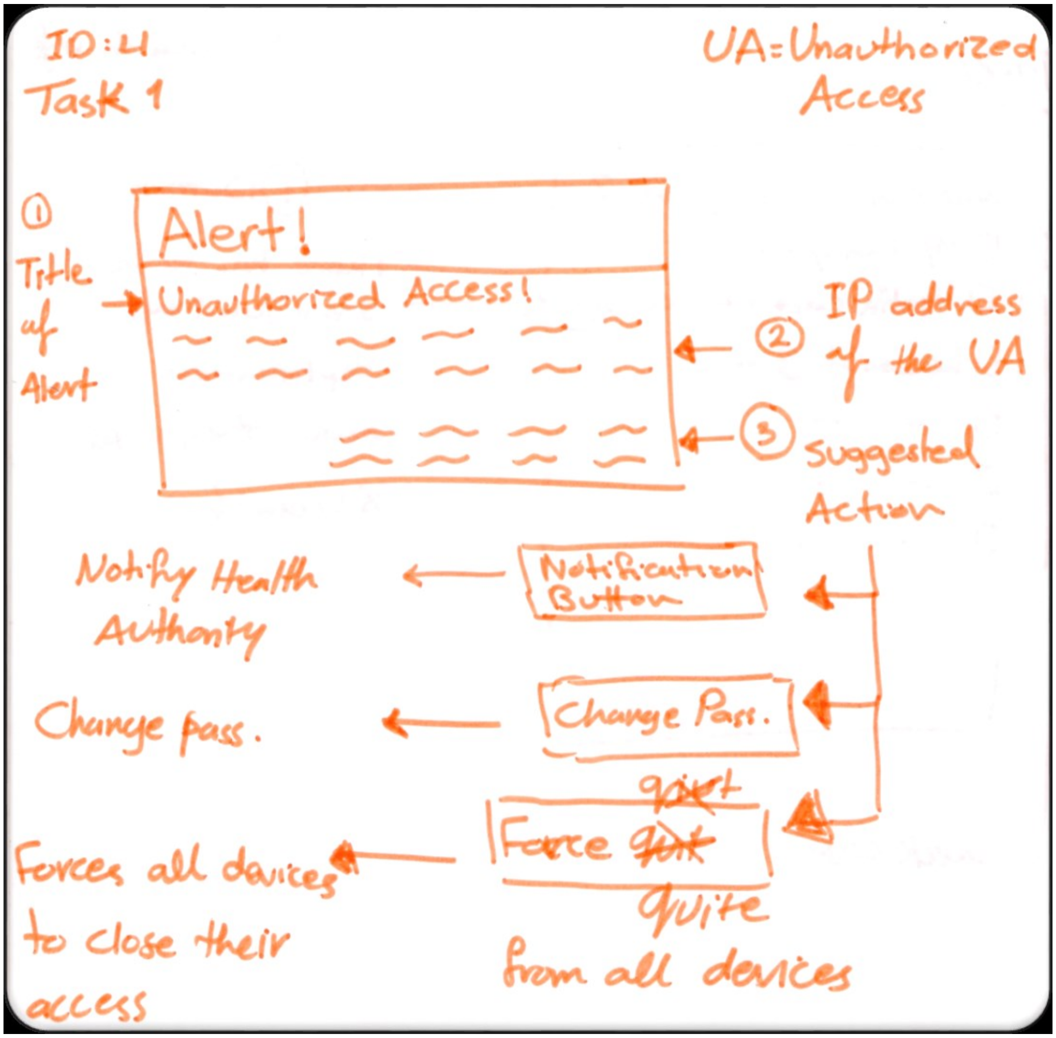


Figure 11. Notification sketch example (Participant ID 4)

- **Who accessed the PHI**

Participant ID 3 raised an important point which is to include the last access time of the unauthorized access, last access machine (a health care provider or agent), and last activity. The time of the last access and who accessed the information will help the end-user recall recent access of the family physician or visit to a healthcare provider. Also, every digital footprint, including the IP address, location, and server, was suggested by Participant ID 7 from the second round.

- **Potential risks and next steps to recover**

The notification should include the next steps to take actions. Participant ID 1 suggested a link to three options: Notification to the Health Authority button, Change Password button, and Force Quit button to log out on all devices that are logged into the system.

A Report Incident button, as suggested by Participant ID 2, is important. The end-user can block the access to their online PHI and sent the healthcare provider a request to reset the username, and, while waiting for the custodian action, the end-user can reset the password, as recommended by Participant ID 4.

The sensitivity of the information that was accessed, collected, or disclosed is vital to know as part of the potential risks.

- **Type of information that was accessed**

Participant ID 6 discussed the point of allowing details on exactly what was accessed and whether or not information was also obtained. The end-user reaction would differ if the information that was accessed was personal information regarding a mental health illness compared to an ordinary health condition, as stated by all participants from the three rounds. All participants from the three rounds focused on the importance of stating the type of information that was accessed because the next steps that should be taken depend on it.

- **Different means of notifying**

All participants from the three rounds discussed the importance of sending a warning through different means, such as emails, texts messages, phone calls, and through the online portal. The nature of the warning requires immediate attention.

❖ **Notification for Defined Purposes: Authorized Access**

As we learned from the Interview Study-Phase 2, any member in the circle of care is considered as an authorized individual to access by the rule of the Personal Health Information Act. The patient has the right, however, to be notified when an agent collects PHI information for defined purposes.

From the list in Table 13, we merged Tasks 1 and 2 as one with different details during the discussion.

No	Privacy Requirement	Task Scenario	Privacy Pattern	Notes During Prototype	Mapping to Privacy Principle
1	Define PHI collection	The patient's PHI is collected for defined purposes	P1 P4	•Who accessed •When •Patient consent	Collection Limitation
2	Define secondary use of information	The patient's PHI was collected for undefined purposes	P1 P3 P4	•Who accessed •When •Why •Patient consent	Collection Use, Retention, and Disclosure limitation

Table 13. Authorized access notification tasks

Task 2 is a subtask of Task 1 because, first, patients (end-users) have to be notified and give consent as the following task.

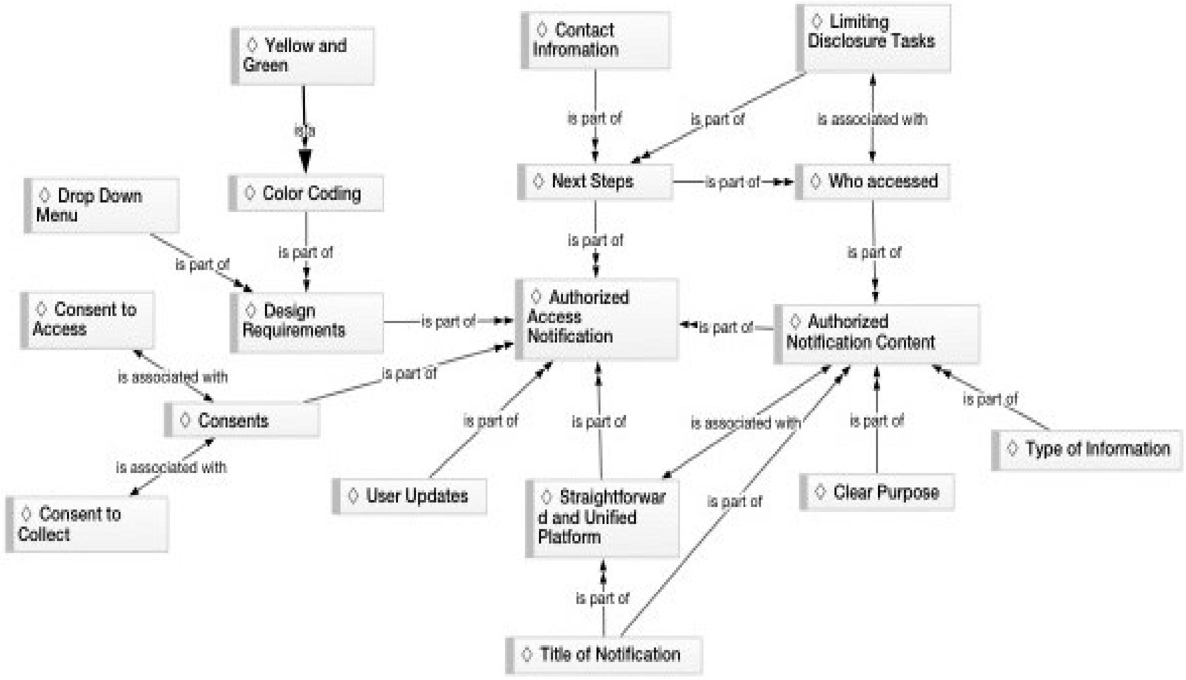


Figure 12. Authorized access notification

- **Design requirements**

Participants ID 3 and 4 from the first round commented that here in this notification design is where the colors, especially green and yellow, play their roles. They should be under the Notification or Alert tabs, where end-users can manage their notifications.

Regarding focusing on the consent that should be collected from the first logging or right after the registration is that Participant ID 6 thinks about the type of the user profile. Participant ID 8 emphasized a design such that the title should be written in a friendly way to avoid frightening the end-user because it should be a low-risk notification.

In the third-round session, Participant ID 10 suggested a drop-down menu that contains all the purposes for which agents can access the end-user profile as a step before sending a notification. In this way, end-users would not be surprised when they get the notification.

- **Notification content**

Participant ID 1 discussed the idea of including clear purpose details, including the type of information they are collecting and what they are going to do with it, to keep the end-user updated regarding the uses of their data if it is changed, as supported by participant ID 2. The type of information they are collecting is going to let end-users decide to give consent or not.

Participants ID 5 commented that it is going to include the same content from the previous notification they designed for the unauthorized access. However, it should be a "straightforward and unified platform."

Stating the purpose is vital in this case. Participant ID 10 from third round mentioned, "I think it would be very valuable for the audience [as it will make it] transparent and make people feel like they're in charge of their record."

  - **Next steps**

It should include links to the next tasks, which limit access to the PHI and consents to access.

Note that from this task, we move to the Information Disclosure tasks, which include setting a pre-defined list of agents, limiting access, and blocking all agents.

❖ **Information Disclosure Tasks**

No.	Privacy Requirement	Task Scenario	Privacy Pattern	Notes During Prototype	Mapping to Privacy Principle
10	Set a pre-defined list of providers and custodians	The patient is interested in specifying a pre-defined list in which a certain number of healthcare providers and agents can access their information or collect them.	P3 P2	•How •What consequences they need to know before applying this feature •When they can and when they cannot	Consent and Choice Purpose Legitimacy and Specification Activity record
11	Limit the list in the activity record	The patient found after reviewing the activity record is that they want to either hide part of the information or want to apply restrictions and limit the list of who can access the information and/or collect them	P3 P4	•How •What consequences they need to know before applying this feature •When they can and when they cannot	Consent and Choice Purpose Legitimacy and Specification Activity record

Table 14. Information disclosure task list

We have combined these two tasks because of the flow that was applied in the discussion during the sessions. We started with discussing the idea of having a predefined list of agents who can access (via authorization) and then start limiting them based on the type of information or the level-of-access that is assigned by the end-user (patient).

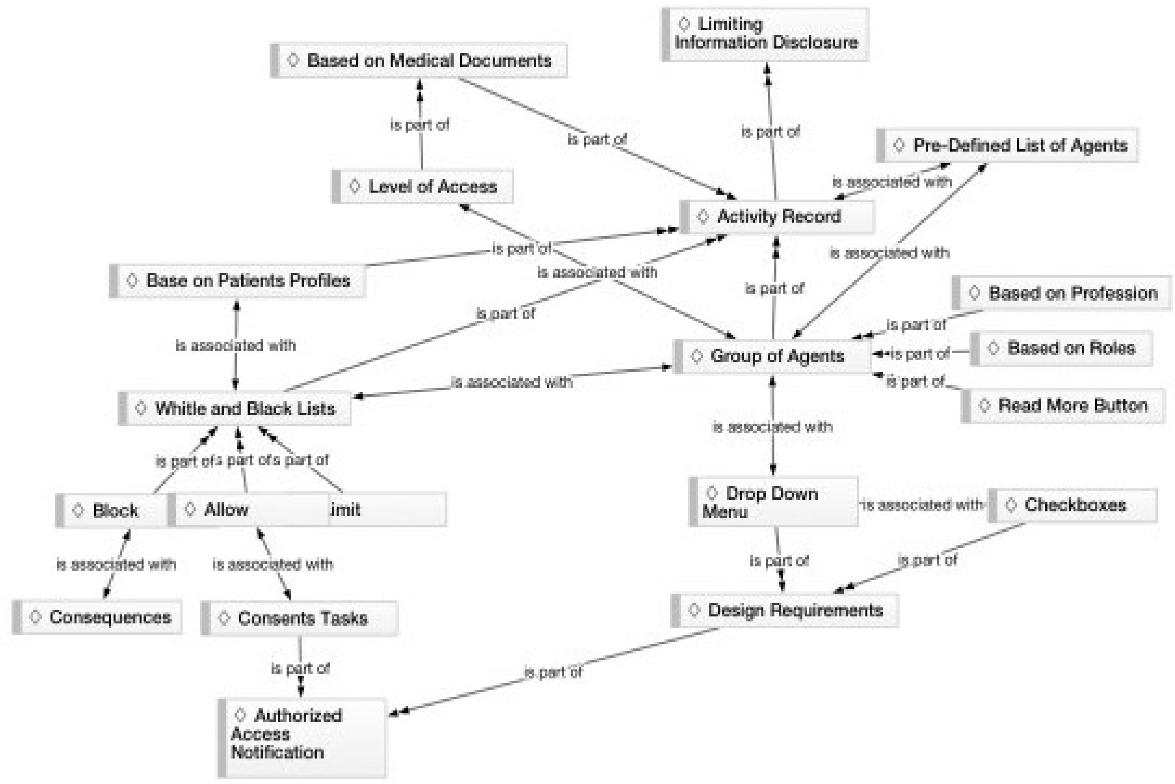


Figure 13. Information disclosure discussion aspects

- **Design requirements and data flow diagram**

Participants from the three rounds share some design ideas but still have differences:

- **Activity record**

Participants discussed the ability to assign a predefined list of agents or limit the agents who can access as part of the Activity Record in the online patient portal. The Activity Record is a list of activities done through the portal. MyHealthNS only displays the type of activity and time and date. Participants wanted to expand the design to fit the privacy-preserving concept that is derived from the legal framework of NSPHIA. They want to design this Activity Record in a way that helps end-users to limit their PHI disclosure as follows:

- **Group of agents**

Participant ID 3 started the discussion with suggesting an Options window where end-users can permit to access to their PHI. The permission should be specified based on groups of agents to represent a predefined list of agents. Participants ID 4 stated, “For me, what I want to check—I want to make sure that I understand the group. If it says, for example, ‘healthcare members’, who are they? I want to know more. It does not have to be names of people. It has to be a role.”

A grouping of agents is suggested to define, limit, or block them via checkboxes and drop-down menus. It should be designed in the form of a drop-down menu organized by groups and then checkboxes beside each agent and an information icon/link to read more about the agent. The grouping, as suggested by Participant ID 1, should be based on their roles, such as nurses, doctors, and staff, or by health organization to help end-users recall recent activities. For example, if the patient had a recent visit to the family physician, then he/she would not be surprised if he/she found a recent activity on the PHI performed by that family physician or their staff.

- **Based on the medical document**

Participants ID 2 and 3 suggested that the level-of-access should be given based on the document itself or on the sensitivity of the medical record. The discussion moved toward, assigning an access or restriction level based on the role of the agent was agreed upon to merge the two design ideas. Therefore, there should be a level-of-access based on the agents and their roles and another level-of-access restriction on the documents as part of the PHI. The idea of grouping agents is better, as suggested by Participant ID 4, instead of asking the end-user to go through each agent and assign a level-of-access.

Participants suggested that they think hiding or limiting access to part of patients' PHI information is going to add a higher privacy-preserving level and deliver a level of control to the end-user. However, adding a "More Explanation" link for consequences regarding choosing to hide or block some of the PHI from being accessed.

By the rules of NSPHIA, some information cannot be hidden, especially in emergency situations. Being such, another link stating a patient's privacy rights under NSPHIA when making actions would help them to better understand the circumstances. It should state under which situations and what types of PHI that cannot be hidden by NSPHIA.

- **Based on profiles**

From the second round, participants discussed the ability to assign a level-of-access based on the predefined profiles. As soon as the end-user registers, the end-user should assign a level-of-access based to the type of agents, who should be linked to the online portal, as stated by Participants 5, 6, and 8.

- **White and blacklist**

From the third round, Participant ID 10, who is involved privacy-preserving techniques, suggested the idea of white and blacklists. The participants of this session discussed the idea of having this feature as a “new classification” of notification, where it appears once the end-user logs in for the first time. The notification would lead to a separate window where the end-user can build on their own white and blacklist, as proposed by Participant ID 10. Participant ID 9 said, “It should give a sense to the patient that, although MyHealthNS is storing their information, [it is] responsible for [the patient’s] safety, [and they] should feel that they’re the ones in control.”

Participant ID 12 suggested adding a note beside each agent to state the purpose of allowing/limiting/blocking access. Providing the reason is part of setting up the whitelist.

For the blacklist, it should include agents that the end-user wants to block from accessing their PHI. This design idea can be applied to the group of agents and the user profiles. Regarding the group of agents, it can be considered as a next step by assigning these group of agents to be in white or blacklists, or the end-user can do it manually to individual agents by clicking “All” or individually clicking in the check-boxes. Regarding the design idea of user profiles, it can be applied as a next step, as well, by having a default whitelist, and then the end-user can uncheck the ones that the end-user wants to be in the blacklist, as suggested by Participant ID 12.

Allowing access should be combined with patients’ consents, which leads to the following tasks:

❖ **Consents**

No.	**Privacy Requirement**	**Task Scenario**	**Privacy Pattern**	**Condition/Note**	**Mapping to Privacy Principle**
13	Obtaining agreement on custodian privacy policy	Patient wants to review the custodian’s privacy policy	P1 P2 P3 P4	•What type of information •Opting in and out •Time stamp •Negotiation	Consent and Choice

No.	Privacy Requirement	Task Scenario	Privacy Pattern	Condition/Note	Mapping to Privacy Principle
14	Obtaining agreement to collect information	Patient wants to know who is collecting their PHR and for what purpose to be able to decide whether to give consent or not	P1 P2 P3 P4	•Type of information •Opting in and out •Time stamp •Negotiation	Consent and Choice Purpose Legitimacy and Specification
15	Obtaining agreement to third party	The patient wants to opt-in and opt-out from an agreement with the third party in case their information is outsourced	P1 P2 P3 P4	• Type of information •Opting in and out •Time stamp •Negotiation	Consent and Choice

Table 15. Consents tasks

We have combined Tasks 13 and 15, and Task 14 is considered as the next step for the Notification and the Limiting Disclosure tasks.

Online consents are considered to be legal documents. Based on NSPHIA, we know when we should provide patients with consents to gain their agreement; however, it does not specify how. We clarified in which "location" the PHI is stored in the previous study, which is already regulated by the Department of Health and Wellness, where all Canadian residents' PHIs are stored locally in Canada.

- **Design requirements and data flow diagram**

It should be in the form of an interactive window. Avoiding the option of agreeing on all the information by clicking on the "Agree" button is going to help end-users focus on the details and be in charge of the agreement's points.

Participant ID 10 from the third round mentioned that the privacy policy agreement should be introduced the first time end-users (patients) finish registering and should also be available in another tab where they have a list of agreements that they can access, as supported by Participants ID 10 and 11.

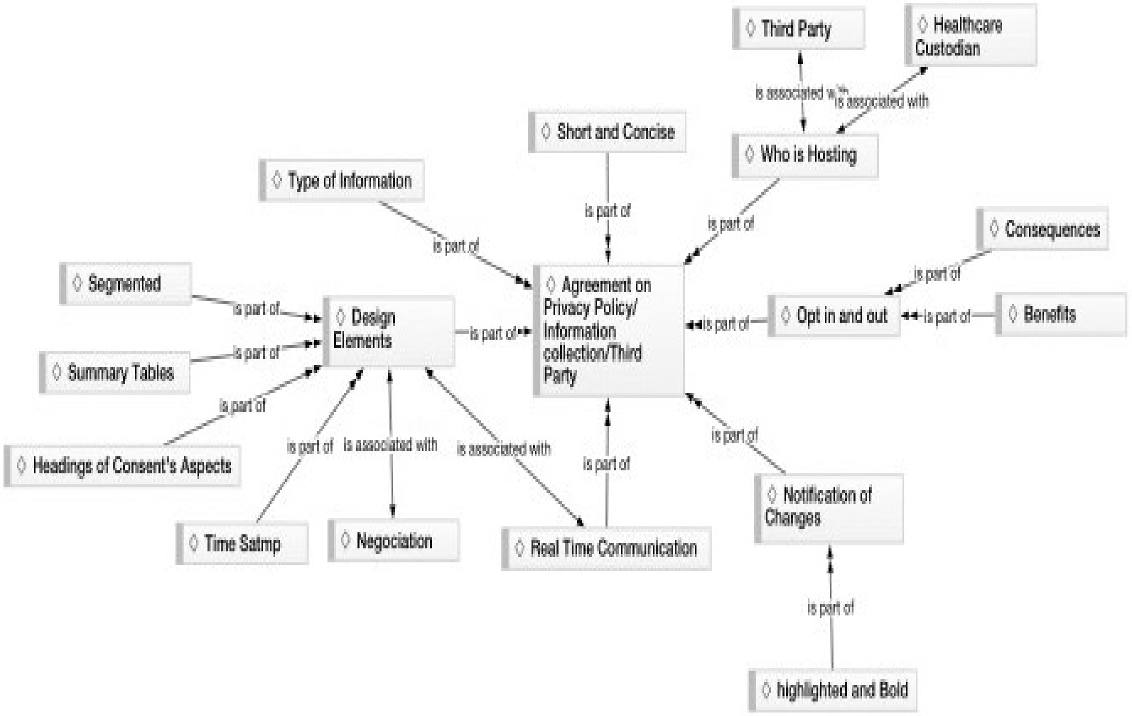


Figure 14. Agreement on information collections analysis codes

- **Short and concise**

Participant ID 3 started the discussion with how the consents should be designed, “short and concise—show me [only] what is important.” All participants agreed on not including everything in one page because “nobody is going to read it,” as said by Participant ID 1.

When the policy or the consent change, a new consent should be signed by the end-user. Participant ID 4 mentioned that the new agreement should show exactly what the changes are rather than the entire document. Participant ID 1 added, “Highlight and/or bold [the updated] text” to make it easier for end-users to identify. Participant ID 5 from the second round mentioned that the system should keep a history of the changes with a timestamp under the heading if the consents. It is intended to help end-users keep track of changes and their gained permissions.

- **Segmented, structured**

It is critical to design an e-consent form that is based on a legal framework but is also short and concise. From this point, participants started a discussion on how to communicate all parts of the informed legal consent but still match some design and usability aspects. They came up with the following design ideas:

First, the entire consent should be listed in sections and tabs that are organized based on the consent sections and divided into sub-points that are not just long lines of texts, as suggested by Participant ID 3. Under these sections, we have checkboxes to opt-in and -out. Where applicable for negotiation, it should provide a Negotiation or Questions button under the checkboxes. An important point is the time stamp to ensure an updated version of the policy is listed under the tab 'Update' and another button to read the full version of the policy, as shown in Figure 15. Participants ID 6, 7, and 8 from the second round shared their experiences and knowledge from the field that end-users do not read long privacy policies due to their length.

Second, the layout of the e-consent should be designed in the form of tables. Participant ID 4 discussed the idea of terms that end-users usually do not understand and have to agree on to be able to use the service. The participant suggested that the first table should be legal terms and their definitions followed by tables of the aspects of the policy; and under each table, there are opt-in and -out buttons that expand to provide more details. A "Send Questions" option at the end of each table should be designed to give the end-user an option to show their concern, as shown in Figure 15. From this point, we discuss the idea of a real-time communication as follows:

Third, Participant ID 5 suggested only including the headings of the consent and a checkbox next to the heading or the title, and if the user wants to read more, it expands for more details. Participant 8 suggested color-coding—the most important parts of the consent or the mandatory ones should be highlighted or underlined or inside a box in red.

Therefore, in all three sessions, all participants agreed on dividing the consent into sections to allow better understanding for patients before they give their permissions. In each session, all participants agreed on the way it should be designed, which resulted in three different design ideas.

- **Live chat or real-time communication**

Having this feature as part of the e-consent provides a real-time communication before deciding to opt-in or -out, which was suggested by Participant ID 4 and also supported by the three other participants in the first round. "That would be great so end-users can decide right away instead of sending emails and waiting for replies," as stated by Participant ID 3.

- **Type of information**

Participant ID 12 from the third round discussed that a section in the e-consent should specify the type of information that is collected and protected by the hosting company in the consent. Patients want to know the type of information that would be collected or shared and how the agent is going to use them (clear purposes) would help them know what they are consenting as suggested by Participant ID 10. The same design concept was discussed in the first and second rounds and recommended to be included in the consent.

- **Opt-in and -out**

Participant ID 1 suggested including the benefits from opting in and consequences from opting out. The extra information can be hidden, and when choosing to opt-in or opt-out, it becomes highlighted.

Participant ID 10 from the third round commented that having consent forms that have been already agreed upon listed in a separate section would make the end-user review it occasionally, and, if the end-user does not agree anymore, he/she can un-check the boxes to opt-out. "That sort of comfort level," as stated by Participant ID 12.

To opt-in and -out using an interactive form delivers a level of control over the aspects of the consent form in which end-users can agree and disagree on. The most common use of the online consent of the privacy policy is usually an "Agree" or close/exit button, which makes the end-user have no control over everything stated. Moreover, the Question and Negotiations button can send questions to the provider to get answers to their questions before they confirm the agreement. A timestamp is included in the heading of the consent and next to the changes 'newer updates' to be able to distinguish original and updates versions.

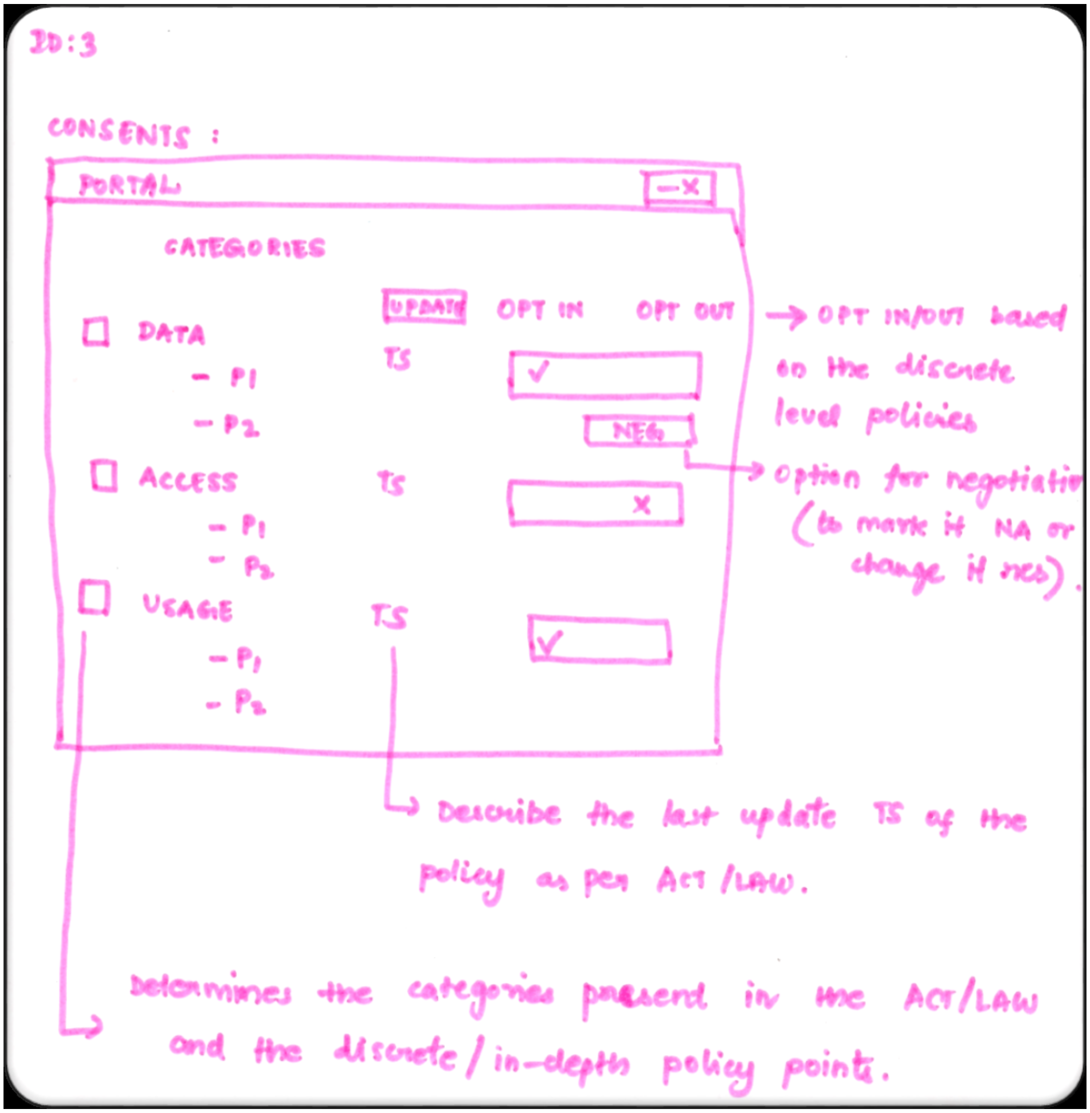

ID:3
CONSENTS :
PORTAL
—X
CATEGORIES
UPDATE
OPT IN
OPT OUT
□ DATA
- P1
- P2
TS
✓
NEG
□ ACCESS
- P1
- P2
TS
X
□ USAGE
- P1
- P2
TS
✓
→ OPT IN/OUT based on the discrete level policies
Option for negotiation (to mark it NA or change it nes).
Describe the last update TS of the policy as per ACT/LAW.
Determines the categories present in the ACT/LAW and the discrete/in-depth policy points.

Figure 15. Consents sketch by Participant ID 3

- **Negotiation feature**

Participant ID 4 stated, “I think when you decide to opt-in or opt-out, you always have questions, and I think having a button to send a question would be beneficial.”

Participant ID 1 disagreed on the idea of having a negotiation feature and mentioned, “It is the manager’s responsibility to contact or deal with these companies hosting the information. What should be done is filing a complaint, which would be received by the managers, and then they [would] have to contact the company itself. I think the company [that provides healthcare or hosts the PHI] will not deal with the patient directly regarding these issues.”

Therefore, the discussion ended with having a question link under the Negotiation button for more clarification Participant ID 3 mentioned that the design should when having a negotiation link is applicable. .

- **Third party policy**

In this case, there is a third party who is hosting the information instead of the health care custodian. The patient has the right to know who is hosting their PHI, and it should be mentioned in the e-consent. The design of the e-consent should be the same but it should be ensured that it states who is hosting the patient PHI in a clear, short, simple way, as indicated by Participant ID 1.

❖ **Data Access**

- **Correcting, deleting, and adding information**

Adding information to the medical record is one of the patient's rights. Communicating this right in a design emerged new ideas, such as the addition being labeled in a way that can be differentiated between a professional medical diagnosis.

Regarding making corrections, it is a right, as well, but it has to be approved by the family physician to be able to upload it online to the online portal. Participant ID 3 mentioned that if the patient thinks that the information is not correct and wants to correct it, the patient has to be able to upload a document that supports the claim. In case the correction is not health information, Participant ID 11 suggested a feature where a "Correct" icon should be listed in the profile setting. Additionally, uploading files should be restricted to medical documents to "not to allow [a patient] to upload 50 different X-rays of [their] toe" to avoid overwhelming the system and the doctor to review these documents, as indicated by Participant ID 10. Participant ID 9 had a different point-of-view, thinking "it should just be limited to a doctor or a health professional." Participant ID 12 supported Participant ID 9 and mentioned that a feature to contact the administration to make changes would be preferred. Participant ID 8 from the second round suggested having the changes appear on the system in a yellow color, and, when it is approved, it changes to green. We believe patients should discuss this idea as end-users and submit their opinions as design recommendation for further research.

Regarding deleting, medical information cannot be deleted when pertaining to a professional opinion of a patient. As a result, input from a physician is going to be nearly completely read-only. When a patient cannot delete professional opinion however, the patient can leave a comment or note that the information is not accurate, and then the physician can comment on that again. This is what we have learned from interviewing a privacy professional, who is a healthcare system expert as well, from the previous study.

6.4.4.2 Post study questionnaire

We have asked participants after each session for a list of open-ended questions to reflect on the tasks, their experiences in exchanging the design ideas, if they had any challenges regarding the tasks or the discussion, and participants' perceptions on the early requirements. In this section, we cover the questions that were asked to the 12 participants from the three rounds.

Q1: What could be integrated as design requirements and what could not? Why?

All participants think that the design elements, features, and structures discussed in the session can be integrated as design requirements, such as pop-up windows, checkboxes, alerts, read more options, etc. A comment from Participant ID 2 explained the way these requirements should be designed:

> "[Design and implementation] should be easy and straightforward since you are dealing with different types of end-user groups, elderly vs. young generations, and literacy levels."

The participant added the point of including tutorials to educate end-users while using the online portal. We learn from this response that we need to have personalized privacy settings for different types of end-users. At this point of work, we are trying to match between privacy from a law perspective and privacy from an IT perspective by creating basic design ideas that cover the law perspective. The next research step is going to be focused on studying different groups of people and adjust the privacy settings according to their profiles. We believe it should be part of the further research that should be conducted, which includes communicating the needs of different end-user groups. However, in this stage of work, we focused on finalizing our initial design guidelines according to the input we get from IT designers of different backgrounds.

Participant ID 11 thinks that adding medical information and uploading medical documents should not be the end-user's responsibility. Reflecting on NSPHIA privacy rights, patients have the right to access, add, remove, and correct any PHI about them in their records. There are some exceptions, such as not being able to correct a professional opinion, until it is reviewed by a healthcare professional, as we learned from the previous study (the interview study). Seven participants out of 12 were satisfied by the details covered, from a legal perspective, to guide them through the design, such as stating clear purposes for collection and trying to comment on the process of designing a privacy-compliant design that all agree upon.

Participant ID 6 had a concern that might not be able to be communicated fully from a design perspective, which is including all information, in case of the privacy breach, in one notification. As a synthesized result from three rounds, we learned that information should be on-demand instead of by default in terms of including them in one design. The design itself should be short and concise but expandable by either “More Information” links or boxes and tables that only appear when clicking for more details.

Q2: What challenges might designers face in integrating these requirements (tasks)? Why? What suggestions do you have to overcome these challenges? From IT perspective or privacy perspective?

Participants had a variety of answers regarding the challenges of integrating the design requirements we discussed in the CARD sessions:

First, designers need to be careful in applying color-coding or combine the color-coding with other visual designs. Participant ID 1 thought that color-blind patients should be considered. As we mentioned from the previous question, different types of end-users’ needs should be addressed as part of the further research.

Second, Participant ID 2 suggests,

> “Do not turn away the users/patients from using your website.”

These tasks should not prevent end-users from completing their main tasks of using the online portal. It is essential to study end-users’ reactions to these requirements for further research.

Next, Participant ID 3 discussed the incomplete picture of the overall roadmap of the PHI flow of information. The participant is specialized in security and privacy, which made his/her reaction focus on the overall data flow, including network, administration’s end, and end-user’s end. We believe it is essential to see the big picture; however, we found challenges in learning the current practices of the flow of the information in NS healthcare systems, which is discussed in the Challenges section in the interview study. We believe that in covering the network, administration and business goals would contribute to the big picture of the context. Our context is limited, as shown in Section 3.3 in Chapter 3.

Q3: What challenges might be associated with these requirements (tasks)? Are they feasible (do-able)?

All participants mentioned that these requirements are feasible if the challenges from the previous question were addressed. However, Participant ID 9 indicated that the tasks should be revised to focus on the flow of the tasks for more comprehension. We discussed this issue, as we already observed it and refined our tasks before using them as input to the next study where participants from different backgrounds, including IT designers, patients, and privacy professionals, are included in one session. For example, the Consent task should be linked to Notification and Limiting.

Q4: What benefits do you think these requirements will bring to the design of online portals or online Personal Health Records?

Participant ID 11 indicated that all the details and the design ideas discussed would help end-users have control over their information and feel more confident that their information is confidential. Participant ID 10 indicated that, "People will have easier access to their health records and build more trust in the online system regarding the information [being] correct, up to date, and provide [a] solid basis for making good decisions about similar situations on the online practice.

Participant ID 2 mentioned, "This would encourage patients to use the website once the benefits of doing so are clear enough to them." We can consider this point as a motivation to ensure including end-users in the next productive sessions because we cannot provide them with all these benefits but, at the same time, not worry them with all of the risky aspects. Participant ID 4 indicated, patients will feel in charge of their data."

Additionally, Participant ID 6 stated, "[End-users] would feel more aware of what is happening with their data and information and feel more in control."

We believe one of the main goals of the research is to empower patients over their PHI, which is a basic concept in privacy and its definition in HCI.

Q5: How do you describe your experience in the "prototyping process"?

The overall impression is positive, and participants enjoyed the sessions:

- "It was very engaging and detailed."
- "It is interesting to know different perspectives of one aspect, such as the notifications and consents"

- “It was helpful for my own research work, also. It is a good way to provide better research ideas.”
- “It is interesting having a group to think with. It brings design ideas and solutions that I did not think of. In other words, [it] open[ed] my eyes on some aspects that I did not think about, which is a great benefit of participatory design.”
- “It [was] an informative talk with valuable outcomes. I hope these design ideas help the design.”
- “It was a very nice learning experience. The brain storming session was enjoyable.”

Therefore, from the initial CARD rounds, we can conclude that sharing knowledge and experience was not difficult because they were all IT designers, even if they had different types of research interests and domains.

6.4.5 Discussion

6.4.5.1 First round

While conducting the sessions, we documented a variety of observations. First, the way the participants were interacting and exchanging the ideas was in the form of building on each other’s designs. They had some time to think separately, sketch designs, and then discuss, which lead to finding that the process of PD is beneficial and led to positive outcomes, which is one of the contributions of the study. We did not face major conflicts with the designs or exchanging ideas except in the following case.

Second, the only time participants did not agree on a design idea was when the discussion led to the point of what next steps should be taken into account to recover from the breach after receiving the notification of unauthorized access notification. Participant ID 1 suggested, “Block all agents from accessing your information, and you can just contact the Health Authority and ask them to get your access again. You have to make an action right away.”

The participant who specialized in HCI and earned a master’s degree in design approached from the end-user’s point-of-view. Participant ID 4 commented, “You do not want to wait for the Health Authority to give you action. Change the password [to avoid further exposure].” Participant ID 3 agreed with participant ID 4 as soon as possible, “You change your password, but [the] admin will still have access to your data.” Participant ID 2 did not agree, saying, “That information is sensitive, and sometimes these kinds of steps [are] going to take some time.

During that time, there goes access to my information, and maybe my health care [also] cannot access my information."

The discussion resulted in the point that the patient has the right to block all access, but, at the same time, we want the healthcare provider to get access. Participant ID 3 said that the alert should be "triggered to both interfaces—the patient portal and the administration office—with more details."

Therefore, the discussion closed on the next steps taken into account to recover from the breach by agreeing on a "Report Incident" button to directly email the healthcare provider with more details and a "Change Password" option but not a "Force Quit" button because we still need the healthcare provider to get access to our PHI. However, when we had such a situation, we found that their discussion led to detailed designs and thoughts about different options.

Third, I learned that giving the participants a sense of how online patients portals are designed is going to help them, especially after the second round due to the reason that three out of seven participants asked questions regarding the design of the interface of the online portal. To help designers in the session, I printed a home page of the system MyHealthNS as an example. It is a simple and generic portal where the current design does not influence the participants' design ideas. I believe it would have been a different situation if the participants were already familiar with patients' portals. NS patients' portals are not widely used, and the provincial patient portal is still under testing (see Limitation section for details).

Another notice is that designers were trying to think about the patients during the sessions, which is an interesting point because all participants tended to do that in the three sessions by asking questions on how a breach notification can be designed without making end-users overly worry. The way they kept the end-user in their minds is an improvement in the field of HCI because of the way designers thought during the design affected the results positively. They were trying to utilize their experience from involving end-users in the design process, which was evident during the discussion.

Next, during the discussion, I did not, as a researcher; want to talk about the rules of NSPHIA, such as the details of these rights, but the discussion itself was taking the direction of requesting more information. For example, an individual right under NSPHIA is to be notified when there is authorized access to the individual's PHI. They started by discussing the differences between this notification and the breach notification (the unauthorized access). Then, Participant ID 1 commented that it should not only be informative but that patients also need to have the option of taking actions, such as blocking some access. Following this, I tried to explain the right of being able to limit access to their information as part of their privacy rights under NSPHIA and moved to the next task.

6.4.5.2 Refinements from the first round

We learned that tasks should be refined regarding their orders. Initially, I divided the tasks according to their categories, including Notification, Data Access, Consents, and Limiting Information Disclosure, and the session would proceed according to the order of the tasks based on the categories. However, we found that the refinement from the first session resulted in re-ordering the tasks to have a more reasonable flow by combing two or three tasks and one primary task that has three sub-tasks. For example, we combined the first and the second tasks: "The patient wants to be notified/informed when there is a detected unauthorized access and unauthorized modification" and "The patient found that his/her information was subjected to unauthorized access." During the discussion, participants did not add more details or have new design ideas to add for the second task because of the context similarities.

The flow of the tasks to discuss during the session was adjusted. I, as the principal investigator, knew the order of the list of tasks because I designed them, but whenever I found there was a need to continue from one task to link it with another task, I did.

Sometimes the discussion lead to moving around between different tasks. However, whenever we started a discussion about a task, I would not let them move until we finished all the notes (see Tasks Takes) I wanted to cover. Before the in-depth discussion of the details and sharing their knowledge, they wanted to make sure that they understood the rules, early requirements, and if there are special conditions. For example, we combined the authorized access with limiting access because they go together as next steps for next sessions. Another example, Task 1, as shown in Table 13, the end-user is getting a notification and dealing with the notification. As a next step, the user has to browse the activity record and start the limiting disclosure tasks, which are Task 10 (setting a predefined list), Task 11 (limit the list of the activity records), and Task 12 (block all agents), which lead to a final notification, as well, with all the changes in the activity record.

6.4.5.3 Second round

We noticed that IT designers from this round were trying to suggest design ideas from their experience as IT designers and end-users of social networking sites. For example, the concept of assigning levels-of-access based on the profile is that when end-users accept access to their pages, they assign a level-of-access to whom is requesting to follow the account, such as friends. These levels-of-access include access all, access some (more detailed settings), and block (do not accept accessing). Participant ID 5 mentioned, "I just imagined [it to be] similar to Facebook. We can have [something] similar to Facebook, [as a] user can have a profile, and then we can have different levels-of-access. For example, your physician, general hospital nurse, etc." Another example is trying to connect the notification window to Gmail notification pop-ups.

Moreover, Participant ID 5 was trying to illustrate based on real-life practices. "I can compare it to credit card security. For example, there should be several options to receive an SMS message, email message, or phone call. So, I should be notified by different means that I, in real-time, could understand that somebody accessed my data."

6.4.5.4 Refinements from the second round

Because participants were having different ideas on what a notification should include from a legal point-of-view, I printed out the privacy breach checklist from NSPHIA information session regarding the content of the notification from a legal perspective to determine if we could communicate it through design. Having a checklist was easier for them to gain a general idea of what exactly the body of the notification should include. During the discussion, we had different opinions on what should be included in the notification and more details listed in an extended version of the notification, as discussed in the pre-design task analysis.

6.4.5.5 Third round

The only point that participants did not agree on in this session was having a contact number to call the custodian when there was a privacy breach notification. Participant ID 10 suggested having a contact method would make the end-user take a step forward in understating the breach because the pop-up window would disappear after clicking on the close window.

An important point was observed during the third round in which Participant ID 9's reactions to some parts of the requirements, as they are not the end-user responsibility even if the other participants agree on the design aspects. For example, the participants did not believe in contacting the custodian in the notification and believe that the notification's purpose was just to let the end-user know that there is a breach. As mentioned by Participant ID X, "I do not know. I do not think it would be, as a user, my responsibility to be in charge of the data."

6.4.5.6 Refinements from the third round

We noticed, during the initial CARD sessions, that the participants spent more time discussing the notification and limiting disclosure tasks, leaving less time for the consents tasks. As a result, we adjusted the order of the tasks to start with the consents and, in some cases, with a mix between tasks ordered in a good flow of steps, not as isolated tasks.

6.4.6 Limitations

One limitation to the study that we thought might affect the results was that participants did not have experience using the provincial online patient portal. I think if they had used it or had experience with it, they would have reacted to these requirements from an experience point-of-view in addition to an IT designers' point-of-view.

Second, the study did not cover the case in which authorized agents collect the PHI for undefined purposes. It is critical because, in NSPHIA, it does not state if this is considered as an unauthorized collection or if it is authorized but in a medium or low risk. A legal perspective should be covered in this case first to build a solid background before discussing the design requirements as privacy-preserving. We could not classify it; however, if we consider it as unauthorized, we would follow the unauthorized access notification and focus on the content of the notification and the next steps. In the content of the notification, we should state that it is for undefined purposes and then lead the end-user for following actions in contacting, limiting, or even blocking the agents who were collecting the PHI for undefined purposes. If we consider it as an authorized collection, we should specify more details combined with more information about the type of information that was collected and what end-users can do to stop such future practices as part of the next steps.

Next, participants discussed the consequences of not giving consent for a part of the information and were asking questions. How would these consequences affect the system itself or the patient or other agents from using the system? I could not answer because it had to be answered by privacy professionals during the study.

6.4.7 Conclusion

We used this analysis, combined with the results emerged from the three rounds of the CARD sessions, to maximize the opportunity of the IT designers to add to the design lifecycle and obtain the legal and feedback from different IT perspectives. All design ideas that were suggested in the first three rounds, such as checkboxes, notification windows, and e-consents, were provided as part of the sketching process to be used in the following Decision-Making sessions.

Our contribution in this phase of the work mainly focuses on high-level tasks analysis of early design requirements that are based on privacy from a legal perspective, which is done by IT designers from different backgrounds, as explained in Table 11. The analyses helped us to criticize the initial requirements and provide enriched refinements and input to the next phase.

6.5 Study Part 2: Proposed Decision-Making Workshops

We propose the Decision-Making (DM) workshop to add to the literature as a cooperative prototyping technique.

The objectives include the following: exploring the scenarios based on tasks and focusing on the flow of the information and how users might interact with each step; communicating privacy-preserving solutions (our proposed solutions with the participants' solutions) in the form of usable designs (i.e., by focusing on the usability of these solutions); and ensuring active participation in the design process of all multidisciplinary teams.

6.5.1 Methodology

We plan to have at least two rounds of the DM workshop. The only difference between the two workshops is the participation of privacy professionals in one session and NOT in the other one to test the hypothesis and to explore the effect of the privacy professionals' early engagement in the proposed privacy-preserving designs.

The benefit that we will gain is that, in the productive session, not only will the privacy professional correct any misunderstandings by our designed tasks and scenarios, but they will also help us recognize any unanticipated requirements and find ways to integrate them. The flow of the DM workshop is shown in Figure 16.

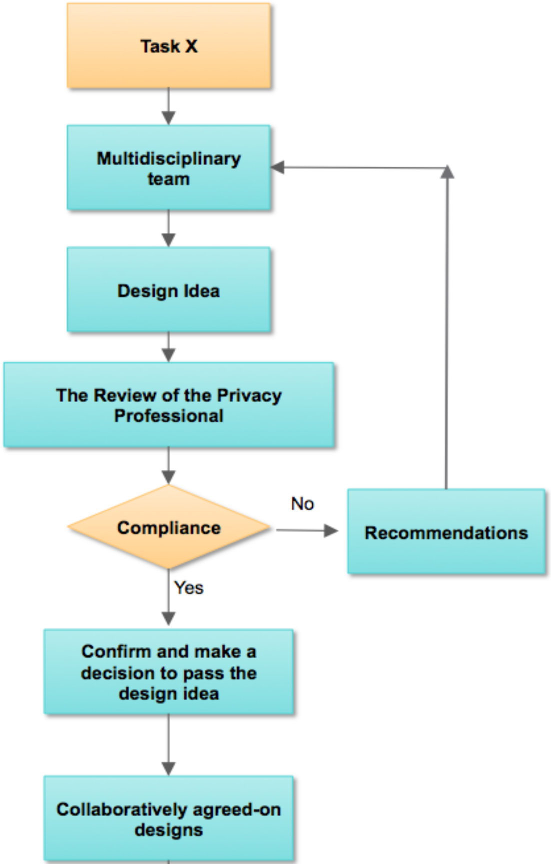

Task X
Multidisciplinary team
Design Idea
The Review of the Privacy Professional
Compliance
No
Recommendations
Yes
Confirm and make a decision to pass the design idea
Collaboratively agreed-on designs

Figure 16. Decision-making cooperative prototyping session

All participants will share a design service that is videotaped, with an audio recording tracking each participant's discussions. The session will start with the first task. All participants will have the same time to think and sketch an idea that covers the task or the design problem. The discussion will start with whoever has a sketch ready. Next, the proposed design will be discussed by all participants and annotated. Privacy professionals will discuss, modify, and identify compliance and non-compliance issues and then recommend ways to overcome them. In cases of non-compliance, the loop starts again; in cases of compliance, where all members of the group discussed the proposed design and agreed on it, they will move to the next task. The anticipated outcome of the productive session as a DM workshop is collaboratively agreed-upon designs that we believe are usable, privacy-preserving, and privacy-compliant. In the session that does not include a privacy professional, we will skip the last step of checking privacy compliance.

We supported the concept of Privacy-by-Design and Participatory Design by involving the multidisciplinary team in the design process.

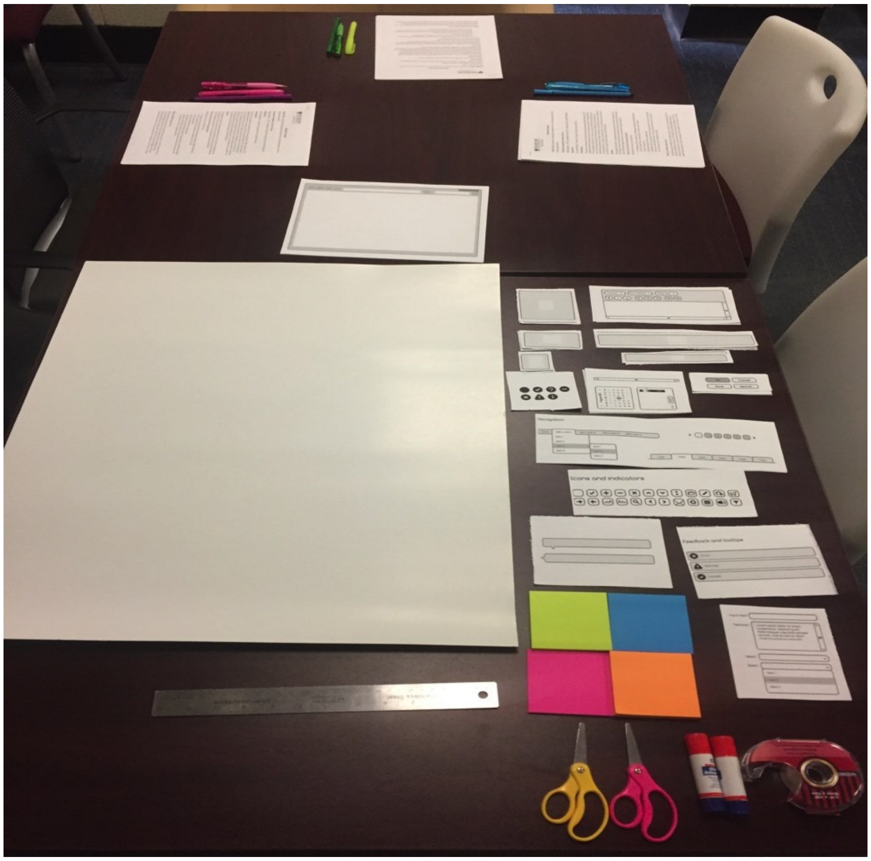


Figure 17. Decision-Making workshop setting

6.5.1.1 Justification of applying the Decision-Making workshop

The proposed decision-making (DS) participatory design workshop shares some similarities with other PD workshops and has differences, as well. First, our DS workshop shares similarities with the PICTIVE method, as both share the idea of having a shared design surface that is videotaped (Muller, 1991, 1997, and 2015). However, they designed the session to include only end-users and developers in separate sessions, but we include different stakeholders who need to focus privacy design and privacy law compliance, and those stakeholders have different expertise and from different domains.

Second, DS workshop shares with the realizing workshop conducted by Weber et al. (2015) the idea of repeated sessions and the number of participants in each session, which is four participants and a researcher to moderate the session. This number was decided according to several pilot studies, which reduce the risks of getting groups that are too large and create the potential of lost discussion and output. Moreover, they conducted the study by separating groups according to their expertise by having one group of end-users and another one with lawyers. We designed our DS session in a way that would include multidisciplinary expertise in one session and then repeat the session with different participants. We want to apply the idea of expanding the concept of end-user participation in one session to come up with collaboratively agreed-upon designs.

Third, we can relate our DM workshop to the general prototyping techniques because we apply low-tech design objects, such as screen layouts and pop-up windows. However, we take the prototyping itself one step further by not only focusing on identifying a problem and suggesting a solution to structuring the designs as co-designers and co-evaluators.

Legal representatives in Europe are included in the last phase of the technology lifecycle right before the releasing of the product (Fliess & Becker, 2006). However, we take it a step further by including the input from the privacy professionals at the early design phase to support both the concept of Privacy by Design (PbD) and provide a high level of privacy compliance.

6.5.2 Tasks

We have applied the refinements resulted from the three CARD sessions. We organized the tasks and design requirements under three main scenarios, as follows:

Scenario 1:

A company (agent) wants to collect/use/disclose patients' information. The company needs to gain patients' consents first. The company has to provide clear purposes for data collection. The patient has the right to be notified when there is a data collection.

Task 1: Design an agreement (consent) to collect patients’ information. We need to consider:

- Data Collection Purposes
- The type of PHI
- Opting in and out
- UI design elements

Task 2: Design a notification of collecting the information. We need to consider:

- “What should a notification include?” list

- Informing the patient of the previous consents
- Color-coding of the type of notification
- UI design elements (pop-up window, confirming buttons. etc.)

Scenario 2:

By using the online portal, the patient can browse an activity record that lists all agents who have accessed the patient’s PHI. The patient has the right to limit who can access their information.

Task 3: Design a feature to help patients limit the list of agents who can access the patients’ PHI.

- Who can access what (the type of information and the level-of-access)?
- UI design elements (e.g. checkboxes, etc.)
- The system detected unauthorized access to patients’ PHI. The patient has the right to be notified in this situation.

Task 4: Design a notification to inform patients when there is a detected unauthorized access**.** We need to consider:

- “What should a notification include?” list
- How we design a high-risk notification
- Color-coding
- UI design elements (pop-up window, confirming buttons, etc.)

Scenario 3:

A company (or agent) has been collecting patients’ PHI for undefined purposes. The patient has the right to be notified.

Task 5: Design a notification for informing patients that their PHI is being collected for undefined purposes**.**

We need to consider:

- What should a notification include?
- Color-coding of the type of notification
- UI design elements (pop-up window, confirming buttons, etc.)
- The patient has the right to review the privacy policy of the company, who is hosting their information, or if there is a third party to be able to provide agreement

Task 6: Design an online agreement in custodian privacy policy. We need to consider:

- Review the privacy policy and how it is represented
- Opting in and out
- Time stamp
- Negotiation steps
- UI design elements

6.5.3 Data Analysis

We collected different types of data during these studies:

- Audio and video recordings
- Pre- and post-study questionnaires
- Our own observations
- Sketches of design ideas

Audio and video recordings were transcribed and coded using the content analysis. An Activity Theory was applied on the video recordings to divide them into episodes to help us understand the process of moving from the problem space to the solution space proceeds in multidisciplinary teams.

For each workshop, we formed a summary sheet to capture themes and key aspects. The data collected from the pre-study questionnaire is used to collect demographic information of the study participants. The data collected from the post-study questionnaires are used to collect qualitative data regarding their reflection on the process of the prototyping and our design requirements.

The data collected from our observation is used to form the discussion and aid the findings resulted from both the CARD sessions and the DM workshops. The sketches represent the output of the workshops and are used to collect design and UI requirements. The study is categorized as qualitative research, as most prototyping methods are.

6.5.4 Participants' Demographic Information

We recruited 18 participants for this part of the study, which include 5 participants in the 2 sessions that includes privacy professional and 4 participants in the 2 sessions that do not include privacy professionals. In each session, we have two IT designers and two patients. Table 16 shows the participants' demographic information.

ID	Round	Gender	User Group	Domain
13	1st with a privacy professional	Male	IT designer	Usability and Mobile User Interface Design
14	1st with a privacy professional	Female	IT designer	Patients Privacy and Software Design
15	1st with a privacy professional	Female	Patient	-
16	1st with a privacy professional	Female	Patient	-
17	1st with a privacy professional	Female	Privacy Professional	Privacy officer and Legal Consultant
18	1st without a privacy professional	Female	IT designer	Usability and Participatory Design
19	1st without a privacy professional	Female	IT designer	HCI
20	1st without a privacy professional	Male	Patient	-
21	1st without a privacy professional	Male	Patient	-
22	2nd with a privacy professional	Male	IT designer	Health Informatics
23	2nd with a privacy professional	Male	IT designer	Health Informatics
24	2nd with a privacy professional	Male	Patient	-
25	2nd with a privacy professional	Female	Patient	-
26	2nd with a privacy professional	Female	Privacy Professional	Privacy officer
27	2nd without a privacy professional	Male	IT designer	Machine learning and mobile design
28	2nd without a privacy professional	Female	IT designer	Health Informatics
29	2nd without a privacy professional	Female	Patient	-
30	2nd without a privacy professional	Female	Patient	-

Table 16. Decision-Making Workshop Demographics

6.5.5 Results

6.5.5.1 First round with a privacy professional

As we have combined tasks from the first part of the study, we started with the consents tasks based on a scenario. The privacy professional is allowed to participate and exchange design ideas and give their feedback at any time during the session; however, the mandatory part is when all participants have input into a design idea, and the privacy professional has to check it for its compliance and then approve it before moving on to the next task.

Scenario 1:

As we have combined tasks from the first part of the study, we started with the consents tasks based on a scenario. The privacy professional is allowed to participate and exchange design ideas and give their feedback at any time during the session; however, the mandatory part is when all participants have input into a design idea, and the privacy professional has to check it for its compliance and then approve it before moving on to the next task.

Scenario 1- Task 1:

When we should design the consents: The privacy professional added important points regarding the consents and their different scenarios:

1. At registration to be able to provide service by collecting different types of PHI to be accessed from one place, such as, in our context, the online patient portal.
2. Different types of collecting information or disclosing, such as collecting PHI from the patient's records for different types of services and diagnosis.
3. To limit access by opting in and out of different kinds of services by being able to limit who can access and collect the information.

For Agreement 1, end-users should not have options to opt-in and -out because it is to provide the service online and the collection of the information is to host the PHI in one place. The privacy professional said this is “because it is not pick and choose. I will agree to this but not that.” Additionally, you need “one signature.”

The privacy professional ID 17 cleared a critical point regarding collecting PHI for the first time to provide service that patients do not have the ability to opt-in and -out from different aspects of the agreement. However, looking at the NSPHIA documentation, patients have the right to limit their information disclosure in consents or revoke them (NSNSPHIA, Section 17 (3 and 5). This is one of the points that we should review with privacy professionals in future work before designing high-fidelity prototypes.

Agreement 2 is where the checkboxes to the consent's aspects are presented and be able to use to opt in and out. Agreement 3 relates to the activity record and its scenario in next tasks. Aspects discussed in the workshop to cover this scenario include the following:

- **Duration of collecting the information**

Not only stating the purpose is important but also for how long the collection process is going to last. Notifying the end-users when the period is done to make sure that the collecting process has ended, and, if extended, the end-user should give consents again.

- **Clear purpose**

The purpose of collecting the information for registration should be simple, such as "we are collecting your name and phone number to call you after registration to schedule an appointment". This type of collection should be clear, simple, and straightforward.

- **Previous experience with e-consents**

Participants discussed their previous experiences as end-users, not IT designers, when dealing with online consents. "I go just next, next, and agree," as stated by Participant ID 15, who is representing end-users as a patient. Participant ID 13, who is an IT designer specialized in usability and mobile user interface design, provided "I just scroll down, and I agree". The privacy professional (Participant ID 17) mentioned that even he/she is responsible of designing such consents, but, when it comes to online consent, "I just scroll down and agree" to be able to use the services. From this point, we discuss the ideas pertaining to different types of consents regarding collecting the information. These cases are not clear enough under NSPHIA. With the help of a privacy professional who is working in healthcare systems, we understand outline the differences. The difference between using different types of online consents and the online consent in our context is that we should design an online consent that end-users can read and comprehend because the PHI that is being collected is considered high sensitive.

- **Informed Consent**

Participants discussed ways to encourage end-users read the e-consent before clicking on the 'agree' button including:

    - **Bulletin points**

Participant ID 14 mentioned the idea of bulletin points in which all aspects of the consent are listed in the form of points. At this point, the privacy professional began discussing how the online consent should be designed and stated that there is a need to help end-users read it without skipping some parts. The privacy professional mentioned that this document is required by the law and stated, “It should be informative to ensure that the patient reads it.”

Including the option of opting out is vital “because if you do not have an option, then it is not consent—it is compelled,” stated the privacy professional.

Participant ID 14 suggests providing 'read more' links next to each main bulletin point to provide more details. In this way, the participants can design an online consent that includes all the information needed from a legal point of view in one page, which would reduce the number of clicks end-users.

- **Checkboxes**

The privacy professional has a different point-of-view regarding opting in and out from aspects of the e-consent for the first type of agreements, as stated, “They’re collecting what they need to collect under law; so you’re not giving the patient the options in this case. Therefore, IT designers need to know when using checkboxes in the design of the e-consent is applicable.

- **A second confirmation**

To make sure that the end-user has read the content of the e-consent, Participant ID 15 mentioned that we need a second confirmation. After clicking on the “Agree” button, we should have a pop-up window that states, “Are you sure you agree?”, and a summary of exactly what is going to be done, such as “Are you sure that you want to allow us to collect your [type of information] for the purpose of [what].”

- **User Interface Design Heuristics and user heuristics**

Participant ID 13 mentioned that it is important to consider UI heuristics to be able to make the designs easier to comprehend by end-users. This point is included in the future work and ways to expand the study.

- **Languages feature and audio sound**

Participants discussed the ability to provide the same consent in different languages, and this feature appears in the bottom of the e-consent with signs representing a letter of the language and an audio recording that reads the e-consent. The languages could be “top three most spoken languages in Nova Scotia,” Participant ID 16 declared.

- **Type of Personal Health Information and who is collecting it**

Participants discussed two essential aspects of the design of the e-consent including the type of PHI that is being collected and who is collecting the information. These two concepts are vital parts of the legal requirements.

- **In case of refusing to agree on the e-consent (next steps)**

The privacy professional discussed the case of an end-user refusing to give consent to the online services. In this case, the e-consent should include the next steps. End-users need to understand the consequences and be provided with a list of options such as a contact number, email address or contact the register office.

- **Link to the privacy policy**

It is essential to link the privacy policy in the same page that patients are working on, as stated by the privacy professional and Participants ID 14 and 15, who are representing the patients' user group.

The sketch that summaries the points that were discussed and reviewed by the privacy professional is shown in Figure 18.

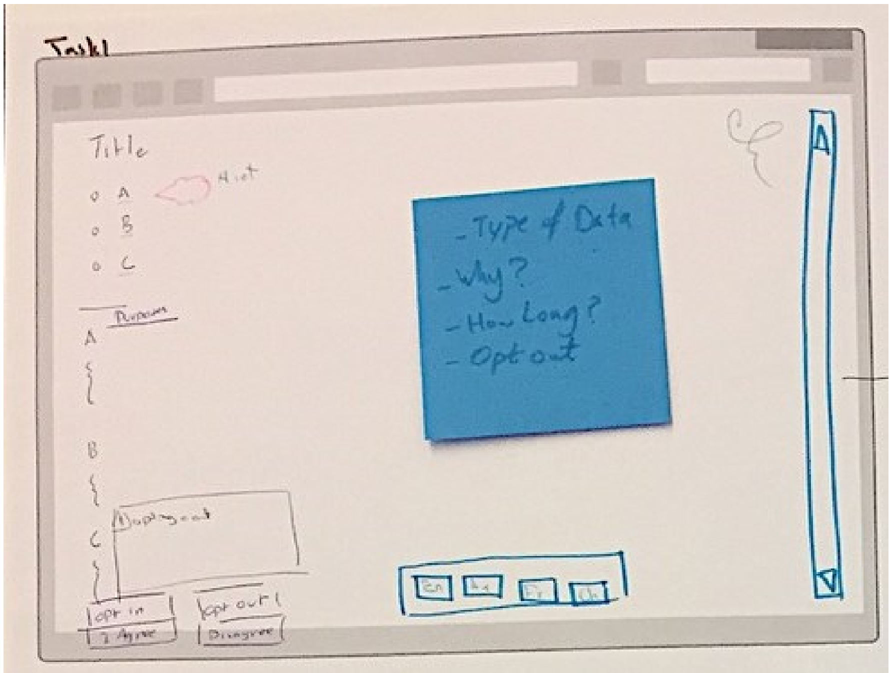


Figure 18. Task 1 sketch in scenario 1

Scenario 1- Task 2:

This section covers the notification of collecting the Patients PHI as a following step of the previous task.

The workshop included aspects that were discussed including the following:

The notification should include that the consent was obtained and the collection of the information has started. It is important to point out that the notification should not be a one-time notification, as whenever there is a collection of PHI, the online patient portal should send a notification.

- **The number of notifications**

Participants discussed the frequency of sending low-risk notifications because they believe the content is dependent upon that, as stated by Participants ID 13, 14, 15, and 16.

Because it is not a high-risk notification, Participant ID 13 stated that it should be listed in the notification box. Participant ID 16, who is representing patients, compared their experience with Facebook—when a friend is starting to follow him/her, they get a notification first followed by a message box.

Regarding when the notification should be sent to the end-user, participants suggest that it should be when the collection of their PHI starts.

- **Type of PHI is being shared and to whom**

Participants ID 13, as an IT designer, and 15 and 16, as patients, mentioned that it is vital for them to know exactly what is being sent or collected about them. An explanation of the type of information would make them feel comfortable with the notification and take advantage of their privacy right.

The notification should list who is going to get access to the PHI.

- **Example detailed scenario**

A patient is registered in an orthopedic clinic and gave consent to host and collect his/her PHI in the online portal that is connected to the family physician EMR. The patient got a notification that his PHI has been sent (shared) to Dr. X, who is an orthopedic surgeon in the bracing department. This detailed example was stated by Privacy Professional ID 17 to help participants grasp the case and sketch the design idea.

We noticed that the workshop participants started deep-questioning and explored different scenarios and want answers to their concerns, which we can reflect on the nature of the DM workshop as a PD technique. For example, Participant ID 15, who is representing patients, had some questions regarding if an end-user got a notification that a clinic X on Street X in their city was collecting their information or got access to part of their medical records. I, as a principal investigator, explained that It is a different task where end-users can get a notification or review the Activity Record and limit who can access their information.

- **The sketch description**

The team has proposed a sketch described as follows:

Covering these aspects, participants started the sketching phase where they could build upon each other's designs. They came up with a notification pop-up window that is also listed in the Alert or Notification box (tab). The notification includes a title that states the message is from the portal and the family physician that is linked to the portal. The content of the notification starts with a sentence that states the date; it then states what types of PHI (a list of A, B, and C) is/are being collected or sent to Agent X (who could be a clinic or a specific doctor) for (clearly defined purpose); it then provides that a copy of this notification is sent to your email; and the last aspect is a link to the Q&A page in case the end-user has questions, and, if they do not find the answer, there is a contact number and email or a message to go and see the registration desk in the clinic for fast contact.

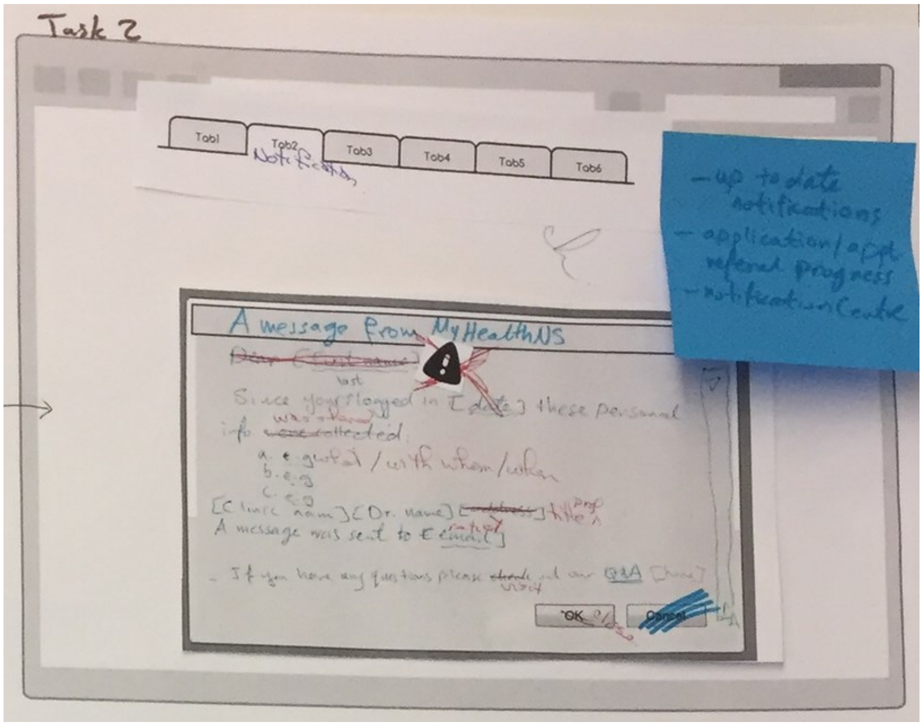

Task 2
Tab1
Tab2
Notification
Tab3
Tab4
Tab5
Tab6
– up to date notifications
– application/appt. referral progress
– notification Centre
A message from MyHealthNS
~~Dear [first name]~~
last
Since your logged in [date] these personal info was shared ~~were collected~~:
a. e.g. [illegible] / with whom / when
b. e.g
c. e.g
[Clinic name] [Dr. name] [~~address~~] title, prof
A message was sent to [email]
– If you have any questions please ~~check~~ visit our Q&A [link]
OK
Cancel

Figure 19. Notification for authorized access sketch

Because it is not a privacy breach and the information is being shared for defined purposes for authorized agents, it should not be in red nor concerning. The participants think that a Close or OK on the window would be adequate.

- **The privacy professional reflection**

The Privacy Professional ID 17 has commented on the following parts of the design:

  - **The type of notification and who obtained access**

The privacy professional mentioned that it should not be in a form "that someone had access to your information but, instead, your information was shared for this purpose to this agent," and because of that you have obtained your referral and scheduled an appointment. The privacy professional focused on the content of the notification and how it should be written.

  - **The notification manger**

The participants discussed the case where the end-user has not logged in for a while. The notification should be listed in a notification tab under a feature called “Notification Center”, where end-users can have a list of notifications organized by dates and can mark these notifications as read or unread. The privacy professional approved this feature as a way of organizing the notifications and making sure patients have read them. The privacy professional commented on having the Notification Center in tab form instead of a drop-down menu because notifications are an essential aspect of privacy rights and “it is more intuitive than drop-down menus.” The Notification Center tab lists different types of Notifications including notifications for appointments, notifications for collecting information, notification of consents, and update notifications.

The participants want to use the “Alert” ⚠ icon to draw the patient’s attention as part of the content of the pop-up notification. However, the privacy professional has a different point-of-view. The online portal is hosting PHI which is considered as high sensitive information. If a patient sees an alert icon in a pop-up window would think that they have a significant health issue, as the privacy professional stated. The alert icon should be avoided unless there is a breach notification. You do not want to use alert buttons for health issues.”

The language that was used in the proposed design in Figure 19 was a concern for the privacy professional. In the design, it says, “Your [personal information] was collected by [an agent name].” The privacy professional was concerned about using the word “collected”, and stated that using “shared” would make it a general language instead of a legal language.

Participants agreed on the point, especially Participant ID 16, who is representing the patients' user group. The participant stated, "Using the word 'collected' made me feel that they are in charge of my information but using shared made me feel comfortable."

Finally, by applying all these aspects of the proposed design that everyone agreed upon, Privacy Professional ID 17 stated, "We know that personal health information is being used accountably, transparently, is being protected, and it is standardized.

Scenario 3 - Task 5: Design a notification for informing patients that their PHI is being collected for undefined purposes.

The privacy professional discussed with participants different aspects associated with privacy breaches. First, a privacy breach notification is sent to the patient through the online portal only if the privacy breach has been confirmed and involves the patient's PHI.

The participants learned that they need to design a notification where a privacy breach is confirmed not a potential of privacy breach. The process of confirming a privacy breach is done by the privacy review office. In our context, the system detects a privacy breach and has been approved by the review office in the Nova Scotia's Department of Health and Wellness.

- **The sketch description**

Participants proposed the following design sketch: a pop-up window that grays or blurs all user interface elements behind. The pop-up window is highlighted in red color and an alert icon ⚠. It includes a title that contains "Privacy Breach". Including the type of PHI that has been breached and how the breach occurred as important aspects suggested by participants and legal requirements. A section identifying what the online patient portal or the healthcare custodian is going to do is part of the recovery plan is essential. "OK" button to close the window and a contact number for more information next to the close icon. The notification has to be listed in the Notification Center as well. The sketch figure is shown in Appendix H.

- **The privacy professional reflection**

The privacy professional started the discussion with trying to avoid a generic design considering that this notification design is a legal requirement to inform end-users regarding a breach to their PHI.

I noticed in this task that the privacy professional was sharing essential information regarding legal ways of notifying patients when there is a breach.

Participants were trying to ask questions and get feedback from the privacy professional on ways to recover, ways to get notified, and getting copies of the breach notice. The privacy professional suggested a print button at the end of the notification "because that is going to be something they may want to take to their lawyer."

The way the notification is structured should not be bulletin points, as suggested by the participants. The privacy professional suggested writing the notification in the form of a letter that contains details regarding what has been breached, for which period, or maybe all PHI in the database, server, or cloud.

The title should be in capital letters stating "PRIVACY BREACH", and all aspects of the privacy breach elements should be listed with more details.

A summary of the privacy breach in a few sentences should be provided in the beginning and then it should go into further details on the same page. It should be on one page, and, because it is to inform the patient, "Close" and "Print" buttons are recommended. For ways to recover or more information, a toll-free number should be provided. Also, a technological next step is included to reset the password. Links to another page where the end-user can copy, or download their PHI should be placed at the bottom as part of the recovery plan. The privacy professional supported the idea of Participant ID 16, who is representing the end-user group and stated, "Can we add any action other than print, maybe contact someone," to which the privacy professional added the toll-free number.

If the information that has been leaked or how it was leaked are not identified at this stage, a sentence clarifying that is essential in the notification, such as "It is still under investigation and wait for the follow-up notification."

Whom committed the breach is not going to be in the first notification. The privacy professional said that is considered as a notice and end-users have to follow up for another detailed notification regarding if there is anything they can do or add to the information from the first notification. "They do not necessarily know at this stage," explained the privacy professional.

Providing the patient with a backup of their information and a link to reset the password were approved by the privacy professional.

I noticed in this task that the validating phase was planned to be a passive phase for some participants and an active one for the privacy professional. It turned out to be active phase for both. They skipped the discussion phase before the sketching phase and started right away with sketching and validating, which I think is caused by the comfort level that participants had with having a privacy professional in the session and after performing two tasks together.

Participant ID 15, who is representing the end-user, shared a similar situation she/he experienced. “I received a breach of information from [a fitness company]. They were very open about it. They stated that we had a breach, and we are investigating this. We are taking it into our consideration.” Participant ID 16, who is representing the patients' user group, as well, asked, “How did you feel when you read it?” Participant ID 15 replied, “It got my attention, and I have read the whole thing…I liked their message because of how they are dealing with my contact information as important information. It was written in a language that showed how much they care.”

An important point was mentioned in the notice that the Participant ID 15 received by regular mail, which included changing the password and a note that “You may want to consider changing the password of other types of accounts if you are using the same email and password.” This idea was approved by the privacy professional to be added to the content of the message. The privacy professional commented on the language that used in the letter. “They used to be very legalistic.” However, now, they are changing to be more common language because it is “for the general public.”

The participant was able to reflect on her/his experience and see the differences of what we discussed in the workshop and what happened in a real-life situation. This can lead to a deeper understanding of privacy rights and what they would expect when there is a privacy breach.

6.5.5.2 First round without a privacy professional

Scenario 1- Task 1: Design an agreement (consent) to collect patients’ information.

The DM workshop participants discussed the following aspects before starting to sketch the proposed design:

- **When**

IT Designer ID 18 mentioned that it is important to provide this agreement the first time they log in or register because it is when the end-user is fully focused on using the services for the first time or returning but before interacting with other UI elements.

- **Before and after logging into the online portal**

The participants discussed the idea of having agreements in a specific order instead of having one agreement. IT Designer 19 started the design idea by having a checkbox under the username and password *before* logging in to give general agreement regarding using the service with one or two sentences. Another agreement with more details is provided once they log in. The participants discussed the idea of collecting personal information, such as phone numbers and email. Patient ID 20 mentioned, “I always get promotion emails for websites that I never give them my consent”. Therefore, giving a general consent to be able to use the online portal is the first step, and then another agreement is provided as soon as end-users log in for more details on the aspects of the agreement.

- **Change settings**

IT Designer ID 19 suggested that the agreement should clearly state that you can change your settings in the future because the consent is asked at the beginning of using the online portal and we need to provide patients with their rights of being able to opt-out from the services at any time. In this way, participants were trying to communicate the legal requirements as design requirements.

- **Purposes of collection**

Patient ID 21 mentioned that clearly stating the purposes of collecting the information and how the information is going to be used is going to “make me feel comfortable using the online portal because I need to know these details, and I want to feel in charge in case I want to stop the collection.” The proposed design gets a positive feedback from the participant who is representing the patients’ user group. Indicating the purposes of collection is a basic legal requirement. Participants at the beginning of the discussion phase do not know that including the purpose in mandatory by NSPHIA. When the discussion got more profound, I, the principal investigator, explained that this is a privacy right under NSPHIA. It is interesting how some legal requirements as proposed at the discussion phase by participants without having prior knowledge of NSPHIA and patients' rights.

- **Agreements center**

Participants agreed on the idea that IT Designer 18 suggested in which we need to have an Agreement Center where these agreements are not appearing every time the patient logs in. Avoiding frustration is important because privacy is not the first task of patients. They are logging in to review their health records or download a copy of their lab tests. Participant ID 18 is a usability and HCI specialist. Trying to integrate the legal requirements as design requirements and at the same time maintaining a level of usability is a great value added to the proposed design by having IT designers from different background in the DM workshops.

- **Privacy settings**

Under Account Settings, there should be privacy settings where patients can change their preferences and review their online consents, as suggested by IT Designer 19 and agreed on by all participants.

- **The sketch description**

As soon as the end-user logs in, there should be an online agreement that lists all agents who are going to be able to access the patients' records, as shown in Figure 20. A "Read More" link that helps the patient to read more on how this particular agent is going to collect and use the PHI should be provided. The link should include the types of PHI that are being collected, duration, who, and the purposes for collection. The end-user can change the settings under the tab "Privacy Settings" with a section called "Online Consents".

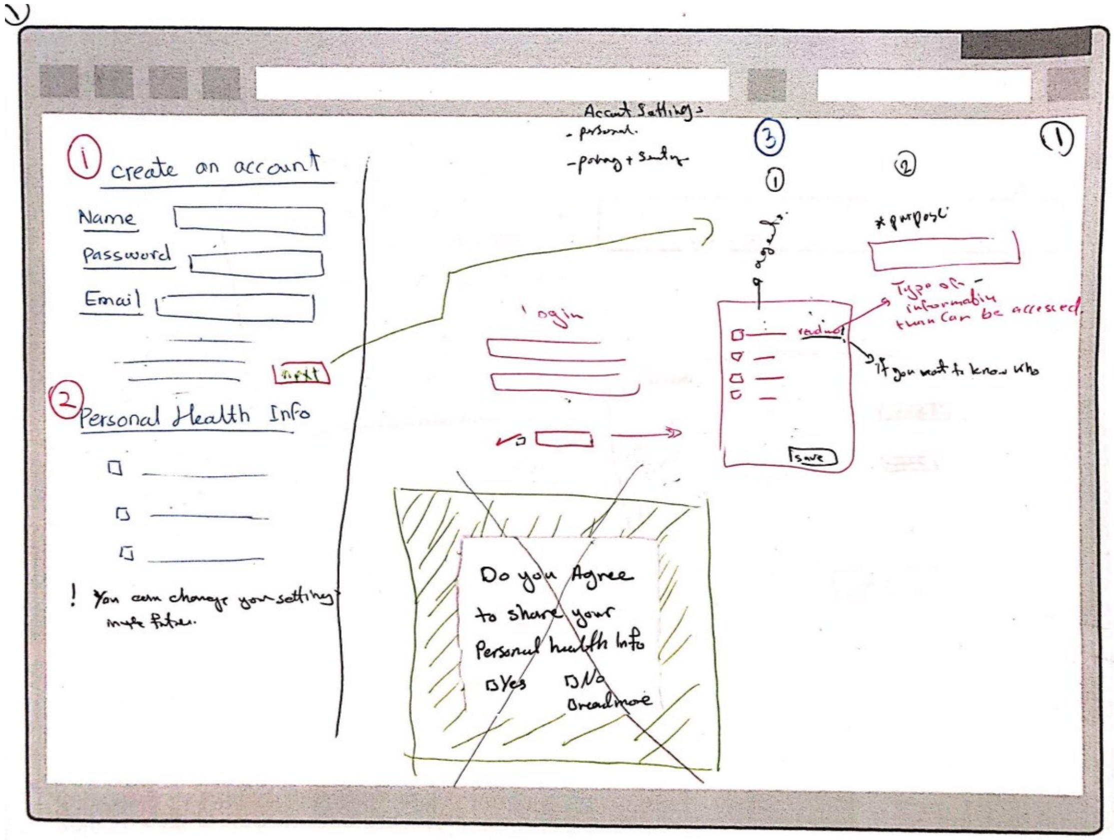


Figure 20. Task 1 in DM workshop round 1 without a privacy professional

Scenario 1- Task 2:

The points discussed here are repetitive from other sessions regarding the type of notification and what the notification should include.

- **Sketch description**

The participants discussed that once the collection started, a pop-up window would appear under the "Account" tab that says "You agreed that [agent] collect patient's PHI [type of information], and the collection has started." When users click on the message, a pop-up window appears that has more information about the agents who started the collection and sharing of information which expands for more details when end-users click on it. It also leads back to the "Settings" page in case the end-user wants to opt-out, as shown in Figure 21.

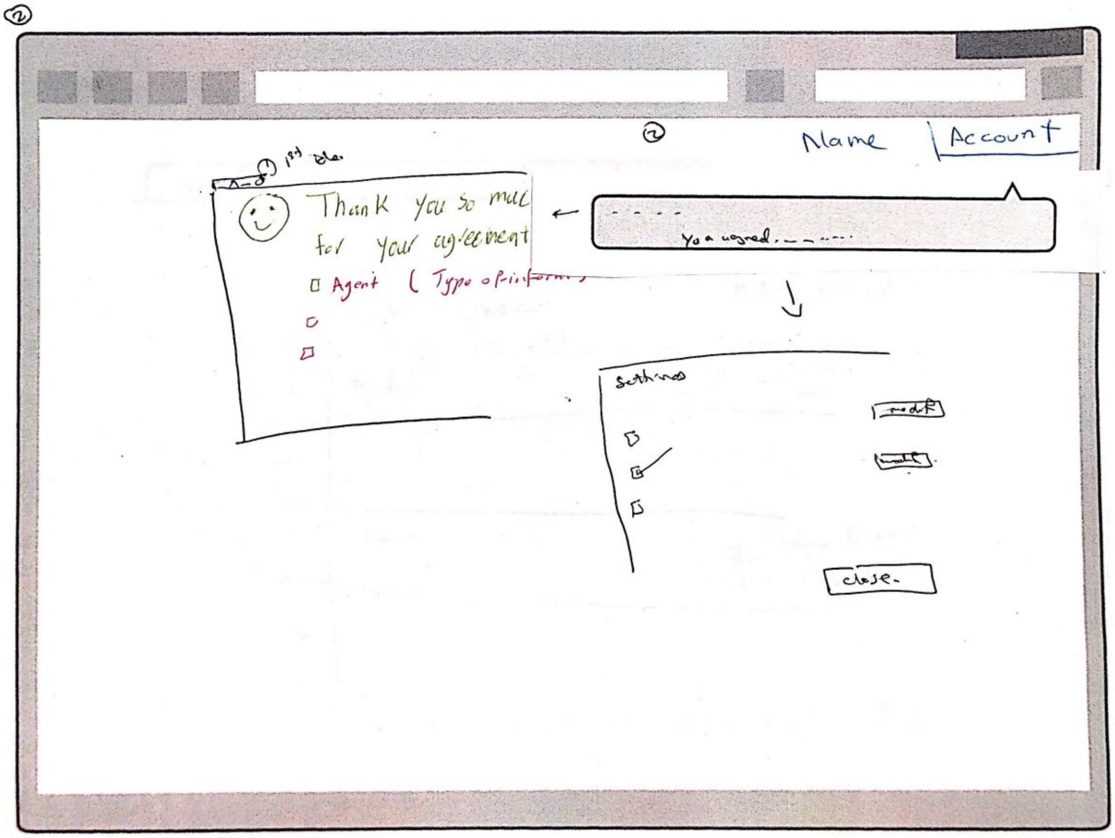


Figure 21. Task 2 without a privacy professional

Scenario 2- Task 1:

- **A predefined list of agents**

Participants discussed the idea of choosing an overall setting to the account itself by assigning a level-of-access, such as the example of Facebook and who can view the account content. For example, choosing only my family doctor or only agents I gave consents to, as suggested by

Participant ID 20, which was supported by Participant ID 21. “I have used this feature before, and I would like to see it in this portal, if possible,” stated Participant ID 20.

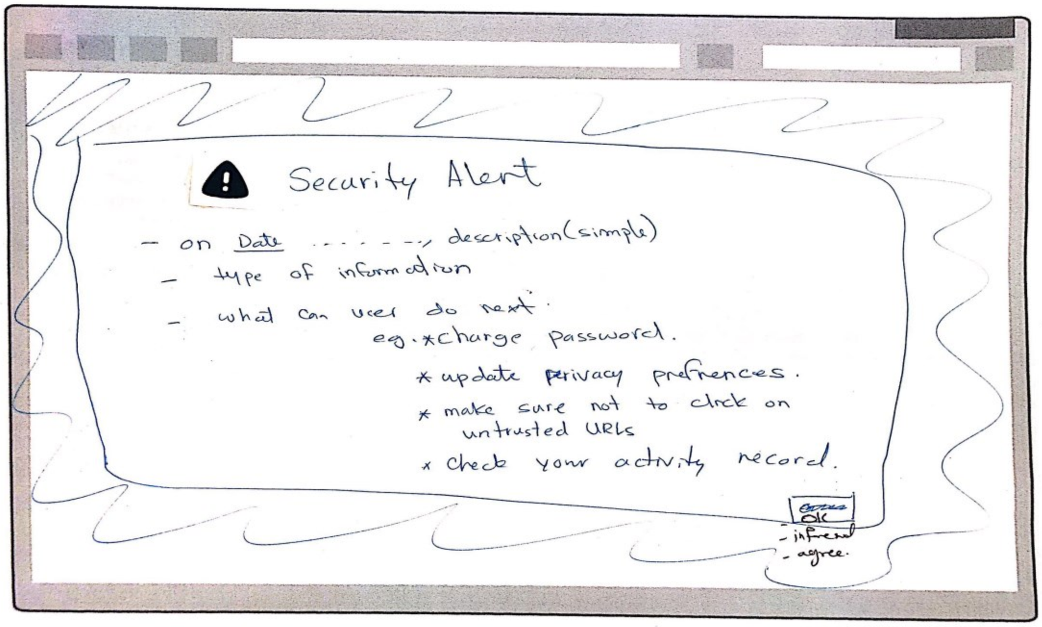
Participants raised an important question regarding the username that the agent would use to access the health recording. “How would I assign level-of-access if the username is a hospital name?” We clarified that it is usually a username and a role in a department—not a general username to represent the hospital name.

Looking at the overall privacy settings of the online portal, agents can be grouped into categories, and then an assigned level-of-access would be given to the group. Users can assign detailed levels-of-access to each and every agent that has access, but grouping them would provide an easier task for the end-users, as discussed by the HCI Participant ID 18.

Participant ID 19 proposed an idea in case the end-user found someone who is not given consent or whom they had never heard of or met before—a “Deny Future Access” button beside each agent in the activity record would help the end-users take actions and limit who can access.

Scenario 3- Task 6: Designing a notification of unauthorized access

The proposed sketch is shown in Figure 22. Participants in this task discussed the same aspects from previous workshops, including different means of notifications, types of data were subjected to the unauthorized access, and next steps the end-user should be taking as part of the solution or recovery plan.



Security Alert

- on Date ...... → description(simple)
- type of information
- what can user do next:
  eg. * change password.
  * update privacy preferences.
  * make sure not to click on untrusted URLs
  * Check your activity record.

Figure 22. Scenario 3 in the 1st round without a privacy professional

6.5.5.3 Second round with a privacy professional

Scenario 1- Task 1:

- **The sketch description**

The team has proposed sketch described as follows:

All participants, as shown in Figure X, built and proposed a design that they all agreed-upon. The e-consent is divided into sections or highlighted aspects that should be included. A "Purpose" section that highlights clearly the purposes of collecting the PHI is the first section in the design including the types of data that will be collected. All sections should have a plus sign ✚ next to the section title, which expands for more details. Under this section, there should be a button to agree for all and a □ symbol to explain the opting in and out process; that is by selecting the "Agree on All" button, all checkboxes will be selected, and it means that the end-user is opting in for all. The green box represents who is collecting the information and what are the consequences of choosing to opt-out. A Revocation from Consent section is listed, which states the privacy right of opting out at any time. Another section is a link to the custodian's privacy policy to help end-users read their privacy rights and cover the legal aspects associated with the privacy policy. "I Agree" and "I Do Not Agree" buttons should be included in the design of the e-consent. "Print Consent" button that summarizes the aspects that have been checked and agreed upon by the end-user should be included at the end of the e-consent. By clicking on the 'Print Consent', a full version of the online consent is converted to PDF that can be downloaded or saved by the end-user.

- **The privacy professional reflection**

IT Designer ID 22 started the discussion by reflecting on their prior experience of not reading online agreements because of either they are long or the way they are written. This point was discussed in both sessions (CARD sessions and DM workshops) and how all participates reflected that they do not read online agreements, especially when there is a lot of scrolling down.

The participants suggested that it should be structured by highlighting or bulletin points important aspects of the consent. However, the group agreed on the concept of designing e-consent based on sections and still including all the agreement's aspects to find a solution between the two ideas. The first idea is that the e-consent is representing a legal document and all its aspects should be included while the other idea is trying to encourage end-users to read it by reducing the amount of text and length.

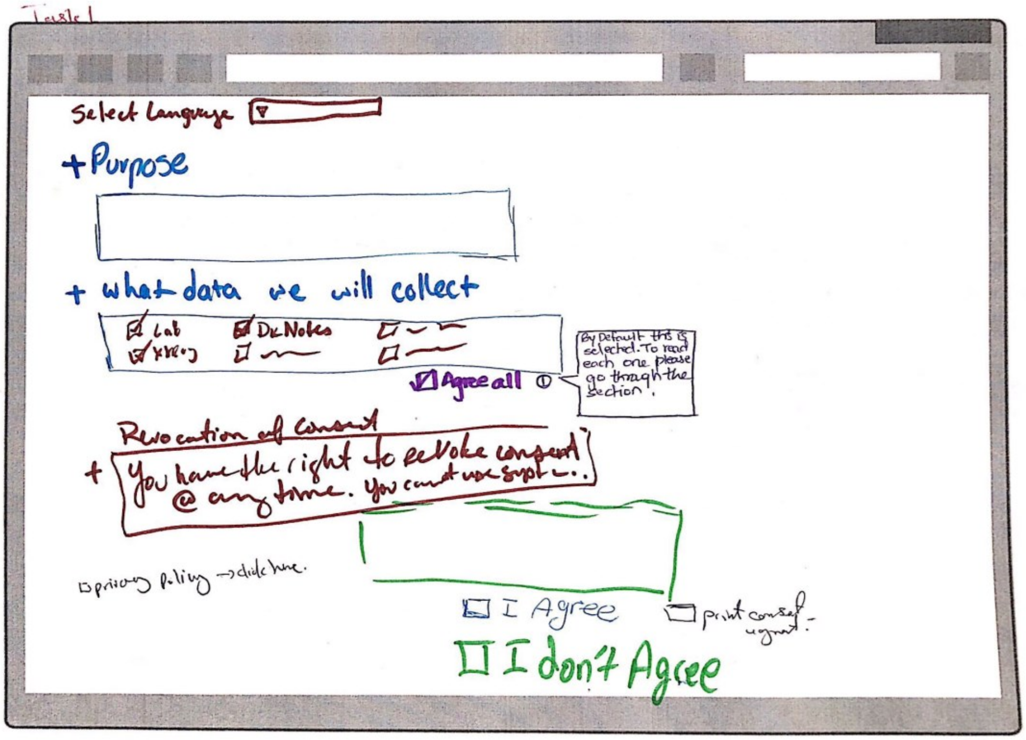

Task 1
Select Language
+ Purpose
+ what data we will collect
☑ Lab
☑ Dr Notes
☑ X-Ray
☑ Agree all ⓘ
By Default this is selected. To read each one please go through the section.
Revocation of Consent
+ You have the right to revoke consent @ any time. You can't use suppl...
□ privacy policy → click here.
□ I Agree
□ print consent signed.
□ I don't Agree

Figure. 23. Task 1 sketch in the second round with a privacy professional

Therefore, all participants agreed on the idea of summarizing the aspects of the agreement under main headings. If the end-user is interested in reading more, he/she can press the plus sign (**+**) to expand the design and read more details. The privacy professional confirmed that it can be organized in this way and still achieve privacy compliance.

Because it is a legal document, IT Designer ID 23 suggested that the consent should not include any legal jargons or difficult-to-understand words. The privacy professional replied, “When we write agreements, they have to be a fifth-grade reading level, and simpler is better.”

When discussing the opting in and out point from consents, IT Designer ID 22 raised a question: “Is possible to agree with some part of the agreement and not the other sections?” The Privacy Professional ID 26 replied, “It is a good idea. It is nice to have the options of the individual opt-in and opt-out to the extent that the project allows.” For example, when dealing with paper agreements, a drug plan assistance program requires full agreement from patients or not the service will be provided "all or not" as stated by the privacy professional. Another type of program is the patients' records repository to collect information for patients to refer to but use the collected information for other purposes such as research. “You might be able to say, well I do not want research, but I do want you to collect. So, it would be driven by the individual program to allow for opt-in and opt-out,” as stated by Privacy Professional ID 26.

From this point, we can see that the opting in and out for parts of the consent is allowed and approved by the privacy professional, as long as the program allows.

The privacy professional added to the design the link to the privacy policy and the “Print” button to download and print the full agreements that summarize all points that were checked.

The ability to opt-out and -in from sharing or collecting information is confirmed for privacy compliance because, as an example, “a lot of patients do not want mental health more broadly shared” Privacy Professional ID 26 declared.

The 'Agree On All' feature under the different types of PHI is recommended by the privacy professional, who stated, “That is an excellent idea. Agree to all. A lot of people probably would not care, but some people might want to be specific.”

The privacy professional agreed on all aspects of the proposed design and added, “The only thing I would add is ‘You have the right to revoke at any time.”

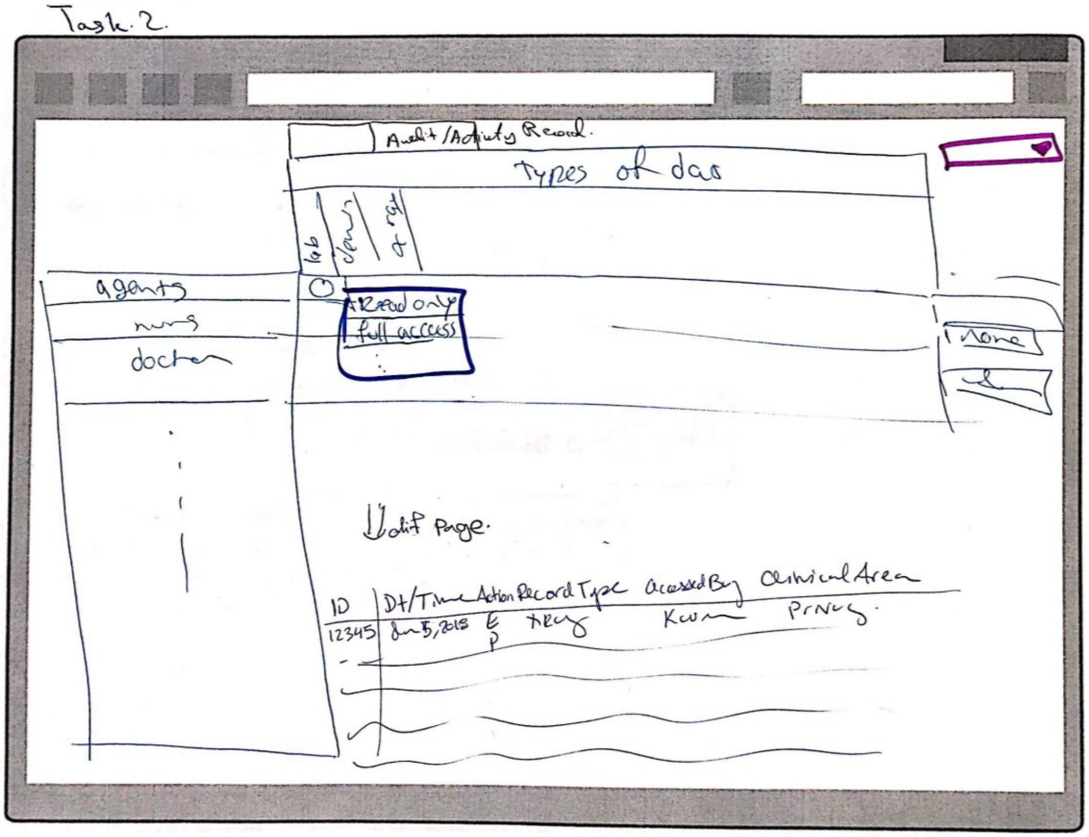
An essential point to mention is that the privacy professional was active through all phases, answering questions, and sketching with the participants (color brown in Figure 23). The role of the privacy professional was not only checking for compliance but engaging also in all phases of the workshop.

<u>Scenario 1- Task 2:</u>

The patient can browse the Activity Record and see who can access the PHI. Patients have the right to limit who can access their PHI.

- **The sketch description**

A separate page for end-users to browse their activity record is designed in the form of a matrix, as shown in Figure 24, to match between the type of data and the role of agents. The first section is a list of different types of PHI, such as lab, x-ray, and other records. Under that, there is a level-of-access, including “Read Only”, “Read and Write”, and “Full Access”. The vertical section is a list of agents based on their roles and names. The intersection between the type of the data and the role of the agent is a button that can show a menu of different levels-of-access. For example, a patient can assign full access to the family doctor. A “Print” button is at the end of the page.



ID	Dt/Time	Action	Record Type	Accessed By	Clinical Area
12345	Jan 5, 2013	E P	Xray	Kwan	Privacy.

Figure 24. Task 2 in second DM workshop with a privacy professional

- **The privacy professional reflection**

Trying to communicate this right, we discussed the task scenario with the DM workshop participants in the following aspects:

Participants discussed the idea of assigning a level-of-access based on the type of PHI to specific agents and their roles. By assigning a level-of-access, patients can limit who can access their information

The privacy professional explained the current procedure if a patient asked for a copy of the activity record. “It is in the form of an Excel spreadsheet, and it could be hundreds of pages. It is organized as follows: an ID, which is generated by the system, date and time, type of record, accessed by, and the clinical area. For security purposes, we do not provide user IDs with the fear that someone could try to hack into the medical record system,” stated Privacy Professional ID 26.

Privacy Professional ID 26 reflected on the proposed design, “Privacy-wise, that is a great idea. The design should not be this complicated. It would be more like demographics. Say you would not have read-write, you would have full or no access to labs, x-rays, that sort of thing. But the general idea of it, I think, is excellent.” Adding buttons to explain more is a good idea, from the privacy professional point of view, because patients have to learn first about their rights in limiting access to be able to use it.

At the end of this task, a question was raised by Participant ID 24 “Is this not against the practitioners' privacy? [Looking at the activity record elements] I can figure out who is working where.” The privacy professional answered, “There is no expectation of privacy as a public employee. Your cell phone, your work assigned cell phone, your telephone, your e-mail [address] is not a matter of privacy.”

The positive effect of having a privacy professional in the workshop is apparent by answering participants' privacy-related questions which helped them think deeply about the proposed design and provide valuable discussion.

Scenario 3- Task 6: Design unauthorized access notification.

IT Designer ID 22 said, “Technically it takes time if they figure out the breach. For example, the very first day they could just only provide, [at] first, one or two items. For example, a breach has happened, and we do not know what data has been accessed. The team can figure out in a few hours how much of the data has been accessed.”

The IT designers are aware that a breach is confirmed after an investigation is completed from both technological and legal perspectives, which usually takes time.

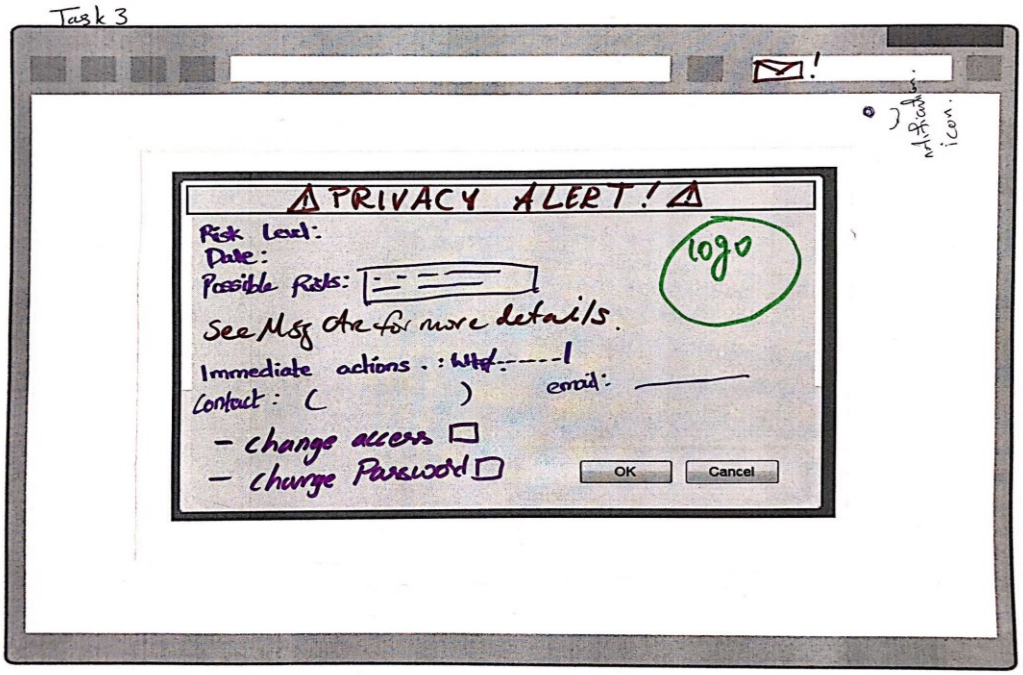
Privacy Professional ID 26 responded that a notification should be sent to the patient “as soon as it is reasonably possible. Even if your investigation has not completed, you do need to notify them that something has happened.”

From this point, participants and the privacy professional agreed to have a series of notifications to provide end-users with details of the privacy breach as the investigation proceeds.

Participants discussed, as well, the point of notification through different means because it is a high-risk situation. As mentioned in other workshops, it is important to suggest technological steps that end-users should take as part of the recovery plan. The healthcare custodian should start the recovery plan as part of their responsibilities under NSPHIA. Participants discussed these responsibilities with the privacy professional and what matters to participants, who are representing the patients' user group, is the two main aspects: how they are going to be affected and what next steps the custodian is going to take to recover from this situation.

- **The sketch description**

The sketch proposed by participants and reviewed by the privacy professional is shown in Figure 25. First, users will be provided with a short notification that leads to another webpage with more details to allow end-users to keep track with changes and updates. The pop-up window is going to be on the main page, and the background is in a blur to get their attention. The notification should include the following: the title that clearly states a privacy breach alert and the hazard alert icon; the risk level; dates of breach and notification; possible risks; immediate actions, including a link to the company official announcement page; how to contact someone authorized to answer questions regarding the details; and an email. An essential part of the notification is the statement that clearly says the patients’ rights in this situation, which is the right to file a complaint with a link to the online form to the privacy commissioner. A logo is included, as well, to make the design look official and a link to change the password. The notification should be bordered in red to reflect the severe type of alert.



Task 3

⚠ PRIVACY ALERT! ⚠

Risk Level:

Date:

Possible Risks:

See Msg Ctr for more details.

Immediate actions . : http:-----/

Contact : (   ) email: ______

- change access □
- change Password □

Figure 25 Task 3 in second DM workshop with a privacy professional

- **The privacy professional reflection**

From a privacy professional's point-of-view, there are some aspects that were discussed with the participants, as follows:

It is important to mention “You have the right to file a complaint to the privacy commissioner office as part of the message.”

Because it is hard to contain all the required aspects from the legal perspective in one short notification or pop-up window, we need to have a link to redirect the patients to a page that contains a full description in the form of a letter.

The IT Designer ID 22 suggested the idea of having a general title in the home page before logging in the system and gave an example of Canada Post. When the company goes for a strike, there is a heading bordered in red in the home page of Canada Post, but still, customers can log in and track their shipments. All participants, including the privacy professional, approved this idea. The participants discussed, as well, the idea of the message center so that the details do not go away when the end-user or patient closes the notification or the notification is over.

6.5.5.4 Second round without a privacy professional

Scanrio1- Task 1: Design an agreement (consent) to collect patients' information. We need to consider:

- **Previous experience with privacy agreements and policies**

We started the session by discussing Tasks 1 in Scenario 1. Participant ID 30 started by sharing her/his experience in dealing with privacy policies and agreements. "They are too long, they are too wordy, and there is no time for people to go through each and every point," Participant ID 30 said. Participant ID 27 commented the only thing that relates to design in making the end-user read is to put the "I Agree" button at the end so the end-user has to scroll down, which does not guarantee that they have read it. Participant ID 30 agreed on that point. As mention before, it is the primary concern of all participants in all four DM workshops and the three CARD sessions.

It is a challenge that should be considered, especially in this context, the end-users are patients who might not be in a condition that allows them to read all aspects of the document. However, it should be part of the next research study because it will help us communicate the proposed design suggestions by our participants in the form of a working prototype and explore ways that end-users prefer that prove efficiency.

- **Structured agreement**

All participants agreed on the idea of not having all the aspects of the agreement in one design page in the form of a letter. As stated by Participant ID 30 to communicate all aspects of the legal document, we need to focus on "the privacy part that entitles the patients' interests." For example, if it is about patient data or how it is going to impact the patient they will be interested to read because it is about them not about the company or the custodian. Participant ID 29, who is representing the patients' user groups, commented by agreeing on the previous point saying, "if it focuses on my interests, I will feel that it benefits the patient not a company" which would encourage end-users to read.

IT Designer ID 28 proposed a solution to this point while discussing in case this is against the rules or legal requirements saying, "Once they do the agreement, it can give a small pop-up with a summary of the main points that they agreed and a link to the full document." At this point, after reaching the final round of workshops, it might not be legal to hide some parts of the agreement.

- **Interactive agreement**

Exploring design ideas that would make patients read these online consents is the interactive nature instead of plain text is important, as stated by Participant ID 30. Cartoons or symbols of doctors and patients or a picture of medical files would make the proposed design more attractive to us as patients, ID 29 declared.

IT Designer ID 28 mentioned, “I personally prefer to read different sized [concise] points and paragraphs.

- **De-identifying personal information and reasons for using the information**

IT Designer ID 27 discussed the importance of including the point that “Your information will be de-identified, and, however it will be used for [collection purposes], it will not be linked to your contact information, such as your name, address, phone number, or your health number.” as a way of comforting the end-user. The participant stated that including this point would help the patient understand that their information is going to be kept confidential, even if somebody is going to use it." IT Designer 28 had experience in dealing with health records and confirmed that, instead of names and ID numbers, they have stars *** as part of his/her lab work.

Therefore, collecting PHI for research is already de-identified as we learned from this participant and the privacy professional from the previous study (Interview Study).

However, in our context, it is not the collection for research purposes. Another point is added to include the purposes of collecting and sharing the information in the form of a simple language that patients can easily understand, as suggested by Participant ID 29.

How the patient is going to be impacted is an important aspect that should be mentioned in the design because it is usually what concerns patients, as mentioned by Participant ID 30.

- **Checkboxes and opting in and out**

An interesting point regarding opting in and out from aspects of the agreement is that a participant, who is representing the patients’ user group, has a different way of thinking about the checkboxes. From an online experience, what end-users checkbox aspect is what they agree upon its content. For example, Patient Participant ID 29 mentioned, “I think the checkboxes could be opting out instead of opting in by not checking to the ones you are okay with but checking the ones you are not okay with."

IT Designer Participant ID 27 suggested, sending a summary of checked aspects of the agreement to the end-user email.

- **Consent for future use**

IT Designer ID 27 offered a different scenario of collecting consents to be gained directly after registration by asking end-users’ agreements of future uses of the PHI and with whom it may be shared. It should be outlined, and, after that, an informative notification should be sent when the collection has started or the PHI has been shared.

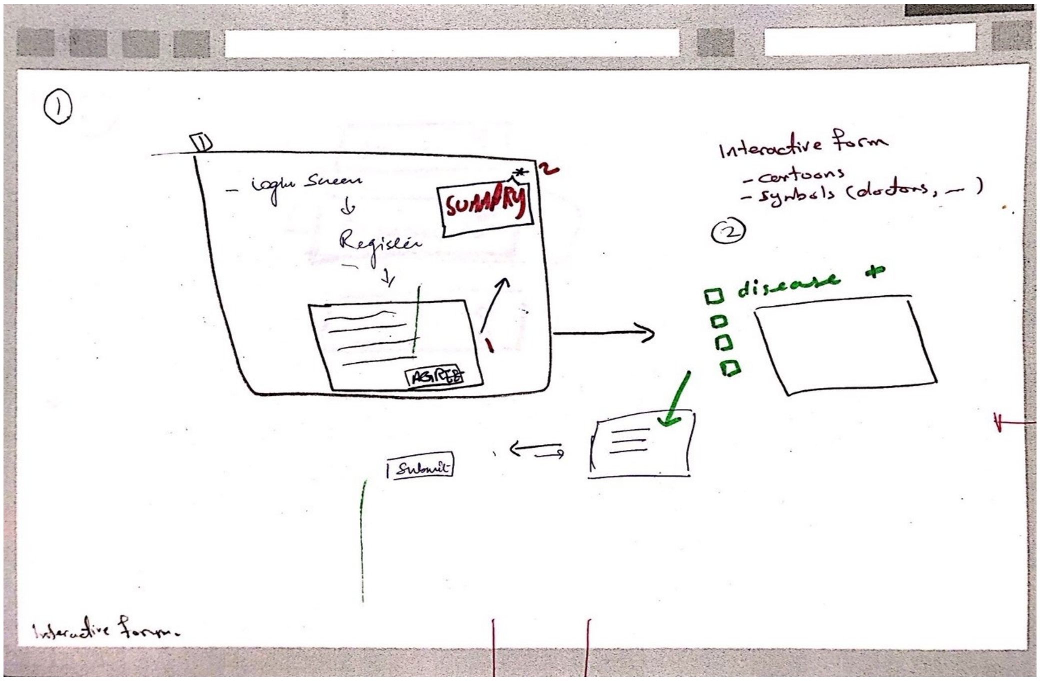


Figure 26. Task 1 sketch

<u>Scenario 1- Task 2:</u> Design a notification of collecting the information

- **Ways of contacting patients and when they get the notification**

IT Designer ID 28 mentioned an important point regarding how quickly the notification should reach the patient: "We do not even know how often the patients are actually logging into their portals, so email is the first point-of-contact." This point does not contradict the idea of using different means of notifying the patient, and, in this case, it is not a highly sensitive notification because it is for defined purposes. They will receive the notification as soon as they log in an informative way.

Participant ID 29, who is representing the patients' user group, commented on the chance to get a notification regarding what their data has been collected for. "I think that would be great." The participant learned that this is part of their rights that they had not known before and liked being able to see the purposes of using their information. We can reflect on the benefits that the participants received from participating in the DM workshop and how the role of educating the public is vital by being able to see the benefits provided by these designs.

- **Dismiss button and review privacy settings buttons**

A quick alert window on the right or left corner with a summary of who is collecting your information and for what purpose could be provided, as mentioned by Patient Participant ID 27. However, Participant ID 30, a patient, mentioned that often these types of notifications are overlooked, and they would click on dismiss just to get rid of the message. Participant ID 28, an IT designer, raised questions regarding the "Dismiss" button that was suggested by Participant ID 27: "Does dismiss mean agree?" It does not. The notifications are just to dismiss this message, as ID 27 replied. Therefore, a "Close" button was the final point that all participants agreed upon.

Another button in the notification should be "Review Privacy Settings" or "Review the Consent" in case end-users decide to opt-out.

- **Managing consents icon on dashboard**

The participants were looking at the home page of MyHealthNS, which includes a dashboard for main tasks that patients can use in the current version of the online patient portal. Participant ID 28 suggested adding both "Manage Consents" and "Manage Notifications" icons in the homepage dashboard. It should have a little symbol in red if there are new notifications or new information collections start.

Patient Participant ID 29 mentioned, "This is way more important to include it the home page. I think it is amazing."

Reflecting positively on the points discussed in the session, participants who are representing patients are impressed by their rights being translated into a design that they can think about and interact with.

6.5.5.5 Results based on the Activity Theory

Broadly defined, Activity Theory (AT) is "a philosophical and cross-disciplinary framework for studying different forms of human practices as development processes, both individual and social levels interlinked at the same time" (Bardram, 1997, p.19). The Activity Theory (Moran, 2006) is currently one of the most fundamental concepts in Human Computer Interaction (HCI) research.

We apply the Activity Theory on our conducted DM workshops by splitting the video tape of the design surface into clips, focusing on which of the six elements of the AT was the main focus of that part of the session.

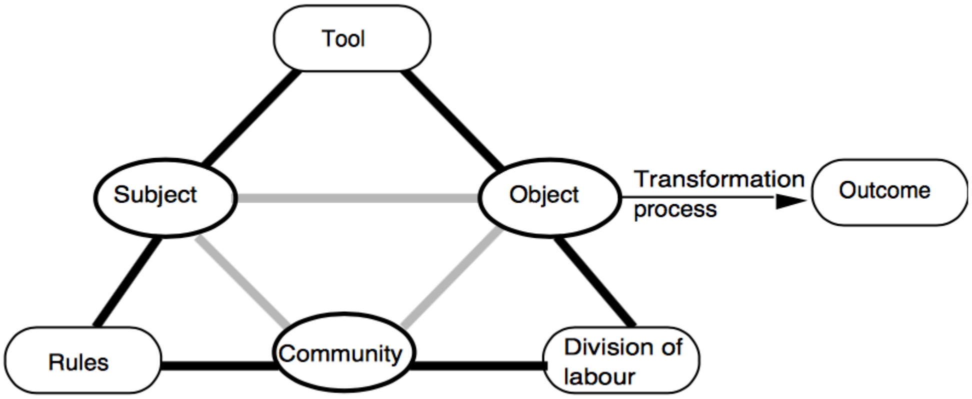


Figure 27. Kari Kuutti model of the activity

The model that we are applying is derived from Kari Kuutti (1992), as adopted from Engestrom’s (1987), which represents three mutual relationships between subject, object, and community, and, later, was expanded to include the tools, rules, and division of labor. “The relationship between subject and object is mediated by "tools", the relationship between subject and community is mediated by "rules" and the relationship between object and community is mediated by the "division of labor"” (Kuutti, 1996).

The reason behind applying the AT is to allow for deeper analysis and answer the listed questions, as follows:

- How the team with multidisciplinary backgrounds interacts;
- What the challenges are and how they overcome them;
- How the multidisciplinary team creates common agreed-upon designs and how the team moves toward the goals of the sessions and tasks;

To answer these questions, we illustrate how our participants interacted and how we applied the AT in our context. We choose one task example and apply the AT to form three cases: one case with a privacy professional, another case without a privacy professional, and last case as an example of the CARD session.

The first two cases represent the between subject analysis and the CARD session represent within subjects analysis through the application of the AT.

- **Data analysis and preparation**

The data preparation was different from the qualitative analysis we performed to describe the workshops and reach the validated or reviewed designs that were agreed upon by all participants—including the privacy professional, or not, in the other case.

First, we used the collected data from both the audio and video recording of the design surface and divided them into episodes based on the tasks and the phases that each task went through to come up with the shared design as the general goal of the task. All tasks were coded, and episodes were created.

Then, we started the comparison process between different cases, and these cases were distributed based on the group. For example, in the workshop that includes a privacy professional, all the tasks were coded based on the episodes of different phases of the design process and compared to the episodes that resulted from the other session that had a privacy professional to distinguish the consistency and identify the recurrence elements of the AT. The same process has been implemented for the sessions that do not include a privacy professional. The final comparison was to compare the two different sessions and outline differences in creating the agreed-upon designs.

We used the AT triangle to support our interpretation of participants' actions during the design activity. It helps in illustrating visually what exactly happened, which elements were the main focus, and what is the main flow of design activity.

We created the full transition between the AT elements that represent the whole design process for all phases starting from the discussion and sketching to the actual proposed design and the evaluation process. However, to understand the episodes deeply, we created a timeline based on the problem space and the solution space to outline the differences between the two types of workshops.

- **CARD session example**

The full episode's description helped us:

- See the general overview of the session's progression,
- A case for us to study and make comparisons to other sessions and
- Data to understand the team progression to propose the design.

The episodes are numbered in square brackets in Figure 28**.**

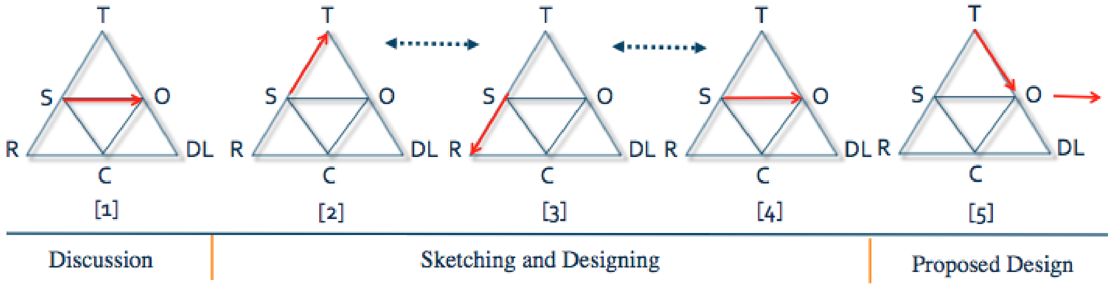


Figure 28. Episodes of CARD session on the unauthorized access notification task

The first episode, [1], mainly focused on the objective, trying to understand and capture all the requirements, and confirming that participants understood by asking questions to clarify some points before sketching. Episode [2] focused on the design elements that should be applied and the tools that are available. In Episode [3], the discussion went back to the details of the rules that should be applied regarding what precisely a design element should include and the number of notifications and their forms. Episodes [2] and [3] were repeated before moving to Episodes [4] and [3], and [4] was repeated, as well, to match between the objective of the task and making sure that the participants covered all the rules regarding the different means of notifications that should be applied. In [5], the participants proposed their design by meeting the goal of the task after applying the design tools.

For all other tasks applied in the CARD session, even if the order of the activity changed, the sketching and designing phases that included Episodes [2], [3], and [4] were the ones that participants were moving from the problem space to the solution space back and forth, which takes a third of the total time of the task. This time was the time when participants were proposing their individual sketches (design ideas) to the group and get each other's feedback.

- **With privacy professional DM workshop example**

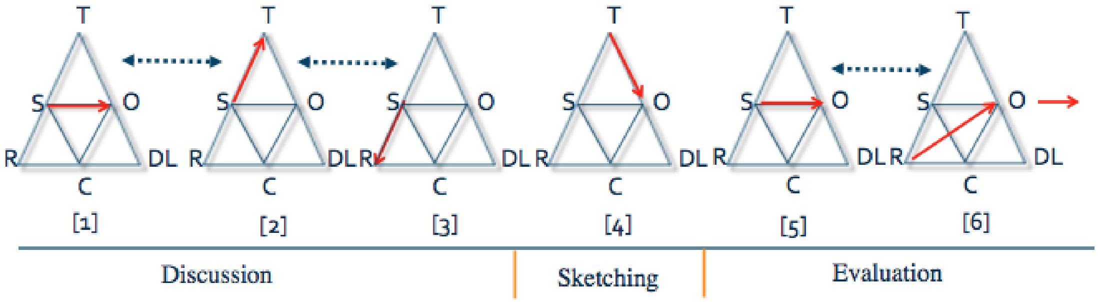


Figure 29. Episodes of DM workshop with a privacy professional

Moving from the problem space to the solution space was only during the discussion sketching phases. This is due to the presence of the privacy professional, who was answering the participants' questions, making them move to the sketching process, and proposing the design that they have no more clarifications to make.

- **Without privacy professional DM workshop example**

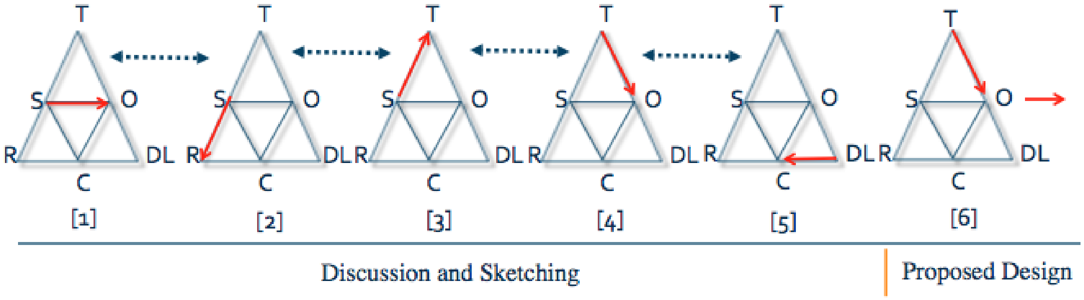


Figure 30. Episodes for DM workshop without a privacy professional

Moving from the problem space to the solution space was distributed for the whole time of the episodes. This might be due to the fact that it is sharing experience and exchanging design ideas but without validation.

We can see similarities in the CARD session that only includes IT designers in terms of the flow of design activity and the workshops that do not have privacy professionals in which there are two types of participants (IT designers and patients) such as in the way that they were moving between the problem space[12] and the solution space. There are still difference between CARD session and DM workshop that do not include a privacy professional on how long it takes them to agree on a design from a time point-of-view.

Using the Activity Theory to gain an in-depth understanding of how co-design activities of multidisciplinary teams proceed to the final design, we noticed that the participation was in the climax during the episodes that were moving from the problem space to the solution space. During the sessions, participants, who were from different backgrounds, shared their knowledge and experiences through different types of participation, including verbal discussions on interpretations of the NSPHIA rules and trying to communicate these rules in the form of design ideas; previous experiences with similar online available websites, such as social media privacy settings; sketching design ideas separately and building on each other's designs; and evaluating

[12] We considered each design task as a privacy problem that needs a design solution.

the proposed designs with the privacy professional to make sure that these designs are privacy-compliant.

Applying the AT has helped us to visualize the activity (workshops) from a different perspective to understand how the participants interacted and which design phases were the main focus of the workshops.

We recommend including the privacy professional in the Participatory Design research to construct design ideas that are privacy-compliant for all the benefits that their existence provided.

We anticipate that the data collected will form interesting and new insights into PD research, especially regarding multidisciplinary teams. Understanding how they interact in specific situations and how they construct design ideas in a multidisciplinary way will reveal new research areas for PD and AT together because both share the same nature. However, investigating multidisciplinary teams in participatory design is new because, from the literature, we can see that different user groups are applying the PD workshops by having each user group alone in one workshop, but we take it a further step by having different representatives in one session.

6.5.5.6 Post-study questionnaire results

❖ **<u>Patients' user group</u>**

1. **What, in your opinion, is the key benefit offered by these designs for online patients' portals?**

Participant ID 15 mentioned:

- Easy designs make it easy for different types of patients
- Thinking about patients and their needs and expectations
- Keeping patients up to date by practicing their rights through these designs

Participant ID 15 mentioned, “Taking my ability to read and analyze the content into consideration” was the main benefit that he/she focused on.

Including patients in this stage was a challenge because we focus on IT designers and helping them to show compliance through our proposed Framework (see Section 6.6); however, getting their insights in this early stage would let other participants from different backgrounds keep patients in mind during the design and the discussion. As part of our future work, further testing by focusing on patients and their need is needed.

Protecting patients' information and giving them the right to be informed about their privacy rights are the two main aspects that were mentioned by Participant ID 21.

ID 29: "Convenience is the key benefit. I can log into the system to look at my data and know that the system is protecting my privacy."

ID 30: "To help patients understand their rights in simple designs."

Therefore, participants who represented the patients' user group recalled positive features and benefits of using the online portal that applies the privacy-preserving requirements we discussed in the sessions.

2. **From the features you have seen today, which ones would make you use the product?**

The participants' responses are summarized in the following table.

Participant ID	Feature
15	The notification center
16	Reviewing consents
20	Knowing who can access and has access to my information
21	Protecting my health records
24	Assigning access levels, access level configuration, and knowing who has access to my records
25	Getting updates on things that I gave my consents to
29	Simple designs that are supporting my privacy
30	Checkboxes, simple notifications, and online consents

Table 17. Patient user group responses on the features that would make them use the online portal

3. **On a scale of one to five, how much do you like this? Why?**

- "I liked talking and listening to the privacy professional. For me, it was so educational about my rights by law," as stated by Participant ID 15.
- "I learned more about my rights," Participant ID 16 said.

- “I like the idea of having all my records in one website. That would save a lot of time,” ID 21.
- “I like how these designs consider the privacy of users,” ID 24.
- “I like it very much because I will not have to set and waste my time in waiting rooms just to check my test results,” ID 29.
- “It is easy to follow and understand,” ID 30

We can see how involving them returned educational benefits regarding their privacy rights, which was reflected by their responses and their design insights.

4. **Having looked at these designs today, what do you remember most about it? What do you recall?**

“I recall almost everything. I remember how it was interactive and how all participants share ideas,” Participant ID 15.

“The icon ⚠ does not mean that I have a health problem. It means that my privacy has been breached,” stated Participants ID 16.

From this point, we can add a hint into the design to avoid the misunderstanding.

“The website is going to connect me with my records and protect my privacy through the designs we thought about today,” Participants ID 21 said.

This response is a strongly positive one because it is not only helping them to have input on the design, but we can also see that they understood the benefits from the proposed designs.

“The pop-up messages for breaches and being able to assign level-of-access to different agents,” Participants ID 30 declared.

1. **Having looked at these designs today, on a scale of one to five, how much would you be willing to use it once it has been refined and launched? Why?**

- “I like them because they are easy to follow. The answer is 4,” Participant ID 15 said. From this response, we can see how much the flow of the tasks that were refined help them to follow a logical flow of tasks based on scenarios as results from the high-level tasks analysis (the CARD sessions).
- “It is going to be easy to access my information and maintain my privacy rights. 5 is the ranking,” Participant ID 20.
- ID 21 mentioned that it is going to save travelling to the doctors to check on blood tests, especially for chronic diseases.
- “I will use it because it is protecting my privacy,” ID 24.

- "It is so beneficial because my information is available, and I trust the government that is protecting my information and the doctor that I am seeing," ID 29.
- "I am happy with how online consents look," ID 30

2. **Do you have challenges in communicating your ideas during the prototyping session with other participants from different areas and backgrounds?**

- Participant IDs 15 and 16 responses were "no".
- "The group was very open to my ideas, and we all worked like a group," ID 21.
- "No. I had some questions regarding blurred ideas, and the privacy professional answered them, such as the level of the language of legal consents and agreements," ID 24.
- ID 25 mentioned, "I arrived a little bit late but this was not a barrier in sharing my thoughts."
- The rest of participants reflected that they did not have any challenges without providing further comments.

3. **How do you describe your experience of "the prototyping process"?**

- "The workshop is very interactive. I liked how it was organized, starting form color-coding for each participant to the design on paper. I do not have experience in paper design, but I like it," Participant ID 15 said.
- "It is so much fun. Communicating and using the sketching materials made it easier for us to imagine the design and share our design ideas," Participant ID 16 said.
- "It helps me understand how should a design for privacy is formed" Participant ID 21.
- "It is constructive process. We built on each other's ideas and came up with good designs," Participant ID 24.
- "A lot of good ideas were shared in the session. I am excited to see how it is going to look in a real design," Participant ID 29.
- "The open discussion is great, and I learned about my privacy rights and NSPHIA," Participant ID 30.

Participants had positive experiences in the workshops, which wa against my expectations as I thought might cause some challenges due to the nature of talking about IT requirements and technology.

❖ **<u>IT designers' user group</u>**

1. **What could be integrated as design requirement and what could not? Why?**

"All what we discussed can be integrated because we are trying to simplify it as we could. Notification manager is a good idea that helps end-users manage their notifications," Participant ID 13.

Participant ID 14 has general advice in that the designs should be simplified in a way that different groups of end-users can enjoy the benefits of using the portal and still be privacy preserving.

"I think they can be integrated, and we will learn more when they are designed in [the] form of a working prototype," Participant ID 18. This participant is an HCI researcher and holds a PhD degree.

"I believe all of them can be integrated, and the overall design is very important to improve users' trust," Participant ID 22.

"They can be integrated with clear summarized information for better understanding and visually designed notifications," Participant ID 23.

2. **What challenges might designers face in integrating these requirements (tasks)? Why? What suggestions do you have to overcome these challenges? From IT perspective or privacy perspective?**

IT designers might face challenges in communicating requirements that are coming from different perspectives, including functional requirements, UI interface requirements, and now privacy requirements, as stated by Participant ID 13.

ID 14 commented on the notification, as well, by designing different types of notifications for breaches, consents, and changes would be difficult. Detailed data flow diagrams should be available.

"Trying to balance between privacy preferences and designing a usable interface might be difficult," Participant ID 19.

"A challenge would be in the limit access page because providing all those options make the page busy and overloaded. Designing light, easy to read pages might be a challenge," ID 22.

"Designers may not be aware of users' privacy preferences. Conducting group interviews with potential users would help," Participant ID 23. Reflecting on the participant response, the next step of the research is to include end-users' perceptions, and more usability testing should be conducted.

"The challenge is to try to design a simple one but conveying all the information," Participant ID 27.

3. **What challenges might be associated with these requirements (tasks)? Are they feasible (do-able)?**

- Participant ID 13 mentioned that the number of notifications should be considered because we do not want to overwhelm the end-users with the amount of notifications that they need to deal with.
- "I guess, all of them are feasible but integrating all of them to 'one' website. I think is difficult," Participant ID 14.
- "How to encourage patient to use the online portal is the challenge," Participant ID 19.
- "I believe they are doable and covering all the privacy requirements would make these designs more privacy-preserving," Participant ID 22
- "All requirements discussed are feasible from a technical point-of-view," Participant ID 23.
  - As mentioned in the previous question, keeping the design simple and trying to include all the requirements is a challenge, as discussed by Participant ID 27.
- "The frequent change in the legislation would make a challenge to keep the system updated," Participant ID 28.

4. **What benefits do you think these requirements will bring to the design of online portals or online Personal Health Records?**

- "Keeping the end-user up-to-date with their personal information and make end-user use their online portal when they know that their data is kept private and they control over their data," Participant ID 13.
  - ID 14 said, "it will give you a well-organized, informed online portal and [usable] as well." This participant was part of the session where they have participants to represent patients and privacy professionals. Making sure that all the design ideas meet users' expectations and way of thinking was one of the main focuses of the workshop.

- “The most important benefit is proposing designs that protect the privacy of patients’ information by default,” Participant ID 18.
- “User interface usability and users would be able to read their consents and get informed without skipping important feedback,” Participant ID 19.
- “Patients’ trust and loyalty,” Participant ID 22 and “Improving privacy and trust of users,” Participant ID 23.
- “Patients will feel more secure in sharing their data because the system gives them instant feedback when a collection process starts,” Participant ID 27.
- “Patients will be well-informed and feel empowered about their rights in healthcare practices. They will build trust and confidence to use the system,” Participant ID 28.

5. **Do you have challenges in communicating your experiences and background during the prototyping session with other participants from different areas and backgrounds?**

- “Absolutely not, with the privacy officer in the room, [he/she] answered all the questions in our minds,” ID 13.
- “No, it was a different experience. It was indeed an informative conversation with the privacy professional to help us design and build design ideas,” ID 14.

All other participants did not have challenges sharing their knowledge and experience during the workshops.

6. **How do you describe your experience “the prototyping process”?**

- “It is the first time for me to be in a Participatory Design workshop. I like it, and it is very informative and creative,” ID 13.
    - “Gathering all the information from people with different backgrounds and putting them together as one design is great. It helps us to analyze and fully understand what we need to do,” ID 14.
- “The experience is wonderful, as I have experience in Participatory Design,” ID 18.
    - “As an HCI researcher, it is the first time for me to be in a participatory Design session. I learned that including different points-of-view in designing for privacy is important,” ID 19.

- "I like the idea of having a group of people from different areas working together to build something. I think the outcome of this collaboration is important," ID 22.
- "My experience is positive and interesting. I gained some knowledge about NSPHIA and patients privacy rights, in general," ID 23.
- "It is a valuable learning experience for me to know the new system and gain understanding of how to keep usability in mind when designing for privacy in health systems. It improved my understanding on how people from different backgrounds think about privacy- and usability-related issues," ID 27.
- "It is interesting to know different views of people from different backgrounds. It was [an] excellent experience due to my area interests of privacy and law," ID 28.

Therefore, IT designers had a great experience in the workshops, which added to their experience in conducting a Participatory Design technique.

- **Privacy professionals**

Privacy Professional ID 17 reflected on her/his experience in the DM session as a Participatory Design positively that is "very interactive and very responsive." The privacy professional liked the way that everyone was interacting and sharing knowledge and experience in one session so the insights can be checked instantly. The privacy professional did not encounter any challenges in sharing knowledge and explaining scenarios from his/her experience.

Privacy Professional ID 26 mentioned that they did not encounter any difficulties in sharing knowledge and experiences and stated, "This was very interesting to be involved to hear other perspectives, and I would use a similar process in my work in the future, where possible."

6.5.6 Discussion

This research phase relates to the overall research goal to understand emerging Personal Health Information Act (NSPHIA) in Canada rules provided to IT designers to show compliance while designing emerging e-health technologies. We found that both the types of sessions lead to positive outcomes regarding understanding legislation, rules and engaging them in the early design process.

We can elaborate on the power of PD methods that we followed in producing empowering designs that are privacy compliance and cover privacy from a legal perspective. We provided the iteration process, which is a basic aspect of PD to enhance designs through multiple steps. This has helped us to show how PD methods are effective, mainly in our context that is interdisciplinary, and there is a need for input and feedback from different stakeholders from different backgrounds.

Participants easily discussed the scenarios and their tasks by identifying important aspects that should be covered. For example, some design requirements from previous sessions are mentioned by avoiding bias by me as a principal investigator. Some aspects were discussed and figured out by participants and were mentioned in NSPHIA rules as well. Participants did not have background or knowledge in NSPHIA before participating. This can show that our participants have strong backgrounds regarding basic design requirements.

The design ideas that were proposed by the DM workshops that did not include a privacy professional share the main aspects of the CARD initial sessions. However, they have some differences regarding the point that these designs received insights from both IT designers and were all agreed upon.

6.5.6.1 Engaging privacy professionals in the study

We noticed that privacy professionals were active and tried to explain any questions that were raised by the IT designers during the workshops. Privacy Professional ID 17 was trying to make sure that IT designers agree on what he/she is reflecting while checking the aspects that were discussed in the designing and sketching phase of the session. This supports the idea that we end up having agreed-upon designs at the end that are checked by a privacy professional for their compliance. In case of not agreeing, the discussion will continue to either clarify some aspect from a legal perspective or find other ways to design the task.

Another positive example is the way Privacy Professional ID 26 reacted to all phases for the workshop, which was engaged in the discussion, sketching, and answering IT designers and patients' questions. Getting instant answers raised the level of understanding and reflected on increasing the level of privacy compliance the designs possessed.

The first round with the privacy professional has outlined when exactly there is a need for patient consent (three cases), and the second round without privacy professional listed one more scenario. These points added by the privacy professional were not listed in our tasks details, and such clarification helped the participants to understand the requirements deeply.

Therefore, we can comment on how having a privacy professional as part of multidisciplinary team can positively affect the level of understanding by IT designers to the legal aspects that are being discussed.

6.5.6.2 IT designers and legal requirements

We have designed the second part of the study in a way that two sessions are in the first round, one with a privacy professional (a legal representative) and the other one without a privacy professional. The session does not only include IT designers but also end-users, who represent patients, to consider their input and engage them in the design process.

The idea of having privacy professionals and IT designers in one session positively affects the resulting designs and minimizes the gap between these two professions. The IT designers proposed designs that relate directly to legal rules and filled their knowledge gaps by having privacy professionals existing in the same sessions and get their design ideas checked. Not only did legal representatives and IT designers get their ideas checked, but, also, end-users representing patients had useful insights into the output designs.

Reflecting on the general research problem, which was the gap between the IT designers and law representatives, designers now believe that they are part of the regularity process instead of the last step of engagement by designing system extensions, such as Privacy Enhancing Technologies (PETs). The participants, especially IT designers, were addressing that the sessions increased their awareness of patients' privacy rights and the application of these rights in a technology solution in eHealth is needed.

6.5.6.3 Engaging end-users to represent patients in the sessions

One participant, who was representing the patients as the end-user group, stated, "I know more now about my rights, and definitely I will use the service." It is evident the raising level of understating regarding patients' privacy rights which would be considered one of the motivations to use the online portal. Involving them in the design process from the initial and analysis phase (as in our case) positively affect the design ideas. Their role in the proposed designs is not less important than the insights that we got from all different stakeholders.

Participant ID 15, who represented the patients' user group, had been active during the workshop and tried to understand in detail and reflect on each aspect. For example, the participant raised an important question during the design of the notification and grouping them under main categories, such as notification for appointments and another category of sharing information. "What is the different between a message and a notification that I would receive? Participant ID 15 asked. The privacy professional answered the question by saying, “[The] message might be a real message from the receptionist or the nurse or the doctor saying ‘Your test results came in. We need to review it and we will schedule an appointment’, this is a message. "[A] notification is to notify you that your personal information has been shared with the specialist.” These detailed and precise questions need a detailed answer from a specialist, which proves the need for having a privacy professional in the workshops.

6.5.6.4 How we applied the flow and types of PD workshops

We can discuss the flow of the workshops in two aspects. We believe applying the CARD sessions followed by our proposed DM workshops has achieved our intended research goals. The way each session was structured resulted in proposing design ideas that are collaboratively agreed-upon. The DM sessions were divided into active and passive phases for participants distributed on the discussion, sketching, evaluation, and proposing of the designs.

The discussion phase starts with the explanation of the scenario and the related tasks. This phase is an active one. Participants were exchanging knowledge and think about how they can design it, with the engaging of the privacy professional or without.

The next phase is the sketching phase, where it contains both active and passive participation. Participants started sketching together and listening to each other's ideas. The following session is the checking session, where it was an active phase for the privacy professional and a passive one for the participants, such that they could relax, listen, and reflect on the design ideas with the privacy professional.

The nature of the PD sessions that we have applied challenges the concept of limiting the gap between the two professions (legal and technological) by incorporating the regulation rules and legal representatives within the initial framing of the design.

One observation from the first session I conducted with a privacy professional is that I waited until they finished discussing, designing, and reviewing with the privacy professional, and then I tried to incorporate ideas from previous sessions (CARD sessions). In this way, I decided to avoid any influence, but, at the same time, I tried to get those ideas incorporated to provide synthesized design guidelines for our framework.

I noticed that whenever the privacy professional did not agree on something, the participants were not very open to contradicting him/her. It is a critical situation because we still need the privacy professional in the session, but we do not want the privacy professional to dominate and force her/his ideas. Thinking of ways to resolve this situation should be part of the next research phase. The checking for compliance should be something similar to heuristic evaluation, and then another round with IT designers to make sure that they agree on the changed design aspects should be held.

6.5.6.5 Contradictions

I noticed that participants who are representing the patients' user group were talking about having only parts that concern patients, such as their PHI, and what they are going to do with it in the second round without the privacy professional. However, the privacy professional in the first round mentioned that it is a legal document that has to be in the form of a letter. A question, here, is raised. If both IT designers and patients do not want to include everything on one document and have extra links for the rest of the information, why can this not be approved by a privacy professional? How can we work on this trade-off or reach a compromise?

I noticed when there is not a privacy professional in the session, the participants spend more time in the designing space. In the sessions that include a privacy professional, they spend more time in the understanding session. I noticed some hesitation at the beginning of the session, but the discussion takes off soon to move on with the points. They were afraid that they would be judged by the privacy professional in the session. This happened when the privacy professional was more active in the first round. In the second round, the privacy professional did not try to participate in the discussion until all participants finished the discussion; participants were open to sharing everything comes to mind without hesitation.

6.5.6.6 Answer to research questions

The research questions to cover the research objectives include:

1. **How do different stakeholders, who are considered to be NSPHIA users who should show compliance, understand privacy law requirements, and apply them during the prototyping sessions, given their limited law background?**

Regarding the CARD sessions, the participants were all IT designers but from different specialization areas. The majority of the time, participants were building on each other's designs, moving toward the solution space smoothly while focusing on integrating the legal requirements as design requirements. They added more aspects to the legal requirements and discussed different cases and examples on how to design these requirements with a simple and easy way without overwhelming the end-user, as they were thinking about the end-user during the sessions, as mentioned in Section (x).

The main tasks were easy to understand, but they raised questions to fully capture the details, which is part of the learning and design processes. The tasks presented to them were in the form of a basic task statement, some points that should be covered in the discussion and the proposed design, which were from a legal perceptive. The participants have different reactions: First, they asked detailed questions, such as the case of asking questions regarding the law itself; i.e. the example of what should a plan to recover from a breach include. Asking questions regarding deep understating of the legal requirement was a barrier due to the extent of not having a privacy professional in the session. In this phase, our goal was to focus on the IT perspective as we design our main contribution to them to show compliance. I, as a principal investigator, tried to answer as much as I could from my initial analysis of NSPHIA; however, some questions remained unanswered. Second, some IT designer participants disagreed with some legal requirements and thought that it should not be the responsibility of the IT designer and the patient, such as the case of IT Designer ID 9. For example, the case of not allowing the end-user to correct their information or knowing where their information should be stored because, from an IT perspective, these points are not crucial to the user. However, the question here is why an IT designer would decide on behalf of the end-user without involving them. This type of contradiction is one of the motivations of having multidisciplinary teams in one setting and mitigates the conflicts. I believe if the IT designers were trained or received an educational session on NSPHIA individuals' rights to build their backgrounds about NSPHIA besides the introduction we missioned at the beginning of the session, it would have made a difference.

Therefore, we believe that IT designers understood the legal requirements but needed some help in clarifying some detailed aspects. The solution to this is having a privacy professional in the session. To relate to the research problem of our thesis, we see how the gap is still there and would be bridged if privacy professionals were included in the sessions to answer the IT designers' questions.

Regarding the DM without a privacy professional workshop, participants represent IT designers and patients. Both have limited to no background on legal requirements. We can see how they share similarities with the participants from the CARD sessions. They raised questions that only a privacy professional can answer and were moving between the task requirements and proposed designs all the time to make sure that they covered as much as they could. Their discussion has raised their knowledge and understanding of legal requirements and how important it is to show compliance, which was reflected in the post-study questionnaire.

In terms of the DM with a privacy professional workshop, the positive effect the privacy professional had on the prototyping process was in form of answering the participants' questions and reviewing the proposed designs. This has helped participants to increase their level of understanding, which is reflected by the proposed designs. The workshop time was distributed in a way that they covered all aspects and discussed all the points with the privacy professional.

2. **How are end results affected by integrating privacy professionals and end-users in cooperative prototyping?**

This question relates to the DM workshops that have a privacy professional.

The proposed designs are validated against their privacy compliance, which meet our research objectives. This is provided through the existence of the following:

The building process of the end results (the collaboratively agreed-upon designs) shows that the privacy professionals have a positive influence. The process involved the input from the multidisciplinary team of participants, who have different backgrounds.

Second, those designs are verified for their privacy compliance. Each component and aspects discussed in the designs are privacy-compliant based on the privacy professional's feedback on these designs. Third, all participants have instant feedback on clarification questions raised because of either of the nature of the task, the detailed aspects of the task, or the UI design elements. This supports our initial hypothesis "Integrating input from privacy professionals at every stage of the design lifecycle will enhance the level of the privacy."

Including patients at this phase would help the design to get their initial feedback on the proposed designs that represent both legal and IT requirements. The designing process focuses on integrating the legal requirements along with the suggested design requirements but, at the same time, getting patients input and feedback regarding these designs. By doing so, we include the feedback of all stakeholders', who are responsible for bridging the gap between the legal language and the IT language and considering who is going to use the final service in the early design phases.

Therefore, we can conclude that these designs not only are collaboratively agreed-upon but also support the concept of the Privacy-by-Design and end-users involvement and support our initial hypotheses "cooperative design that involves stakeholders from different backgrounds lead to outcomes may be substantially better from what purely IT-based designers might design" and "Integrating input from different stakeholders along with end-users from early design phase will increase the level of usability and help in understanding their needs."

3. **How do multidisciplinary teams in co-operative prototyping sessions affect the process of constructing ideas**?

Answering this question is related to the analysis we have done in using the Activity Theory, which shows how each type of PD session is applied and how the multidisciplinary team of participants move from the problem space (tasks) to the solution space (proposed designs). All groups came up with collaboratively agreed upon designs, but the process of constructing the designs and the types of designs (validated for privacy compliance or not) differ based on how they acted through the discussion, sketching, evaluation (in case of the existence of the privacy professional), and proposed design.

4. **How does Participatory Design research affect the outcome of co-designing by different stakeholders?**

The nature of the PD sessions that we have applied challenges the concept of having the two professions (legal and technological) gap by incorporating the regulation rules and legal representatives within the initial framing of the design. We have applied the CARD sessions as high-level task analysis and supported by more detailed formal PD technique, which is our proposed Decision-Making workshops. The way that these sessions moved from active to passive phases helped our participants to come up with the collaboratively agreed-upon designs that are usable and privacy preserving.

6.5.7 Decision Making Study Limitation

One limitation of the study is that some aspects of the designs are not validated for their compliance. However, we have made comparisons and conclusions based on the other aspects that were validated by privacy professionals. These sessions revealed many design ideas and should be used as input for future work to apply formal validation and evaluation research techniques.

We have the idea of not being able to opt-in and -out for aspects of the e-consents, as stated by Privacy Professional ID 17, "we only need one signature, and it is already determined by law who can access." However, it is the right of individuals to limit and agree on parts of the agreement but not all, as it is regarding the collection of their information. This point needs further discussion and review by privacy professionals in future research.

The sample population that are representing the patients' user group is not wide. We only recruited a young generation to participate in the study because of recruitment difficulties and time restrictions. We wanted to include their initial thoughts from the planning and design lifecycle. However, we need to conduct further research on different user groups based on their ages and type of health conditions to evaluate the usability of these proposed designs and framework.

As a result of a time limit per each workshop, we could not cover all the tasks in each workshop. It was hard to schedule all participants from different backgrounds (a privacy professional, IT designers, and patients) in one session that lasts more than 90 minutes. The tasks that were not covered in the workshop that has a privacy professional in the first round were covered in the second round.

The resulting agreed-upon designs are only evaluated if they are privacy-compliant but still are not evaluated for their efficiency, effectiveness, ease of use, and satisfaction. I believe the designs should be evaluated first when they are in the form of high-fidelity prototypes, and then test it with end-users to measure their usability. These designs were generated by applying the PD methods, which showed their effectiveness to create powerful design insights into the privacy-compliant user interface in e-Health that go beyond the traditional methods, such as interviews and focus groups.

We had an original plan where doctor's office administrators and NSPHIA representatives should be present in the sessions to get their feedback; the lack of interest to participate was a barrier. We need to iterate the designs with a wide range of user groups to be able to gain more in-depth analysis and agreed upon designs.

6.6 Aggregated Results from all Sessions

6.6.1 Privacy-Preserving Framework

In this section, we are synthesizing all the information that we build step by step in our research methodology to construct the privacy-preserving framework that is based on Nova Scotia's Personal Health Information (NSPHIA).

For each privacy right or design requirement, we are going to include the following requirements as privacy-preserving framework elements as shown in the following Table 18:

Title	Privacy Design Aspect
Privacy Right	Quotes of the privacy right under NSPHIA
Reference to NSPHIA	Linking the design aspects to the NSPHIA legal sections
Legal requirements	Additional legal requirements
Privacy requirement	Detailed scenarios of notifications
Design requirements	Proposed design aspects suggested by participants
UI design requirements	Proposed user interface design elements suggested by participants
Privacy Patterns	Relating to the privacy patterns from Chapter 4
Task/data Flow	Suggested task flow
Mapping to ISO Privacy Principles	ISO 29100 privacy framework principles
Challenges	Challenges mentioned by workshops participants
Additional Consideration	Extra thoughts, observations and comments
Verification by privacy professional	Privacy professionals reflection

Table 18. Privacy-preserving framework elements

Each aspect of the framework is discussed in details throughout the thesis. The following tables represent a summary of privacy design requirements:

1. Notification- Unauthorized Access	
Privacy Right	"The custodian is required to notify individuals at the first reasonable opportunity if the custodian believes on a reasonable basis that personal health information was stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and as a result, there is potential for harm or embarrassment to the individuals" (NSPHIA, 2013)
Reference to NSPHIA	Section 69 of NSPHIA
Legal requirements	The unauthorized access notification could be notification for: • Unauthorized sharing • Unauthorized modification (by healthcare agents and/or third parties) • Unauthorized disclosure (from inside or outside Nova Scotia)
	• Who has access or accessed • What type of information • From where • A 'Report Incident' button to file a complaint • The privacy right has to be included which is the right to file a complaint with a link to the online form to the privacy commissioner • A written policy of way of containing the breach should be included
Privacy requirement	The design should include the following: • A brief summary of the breach • Potential risks and actions are taken by the custodian to recover (e.g. a contact number, an email address, the location of information desk) • Possible risks • Statement of immediate actions taken by the custodian and the end-user • Suggested actions are taken by the end-user (both technical and privacy rights) • Contact number
Design requirements	The design should include the following: • Different means of notifications (a phone call, an email, on the online portal and an official letter) • Considering the number of notifications (based on the results of the breach investigation and for usability purposes) • Concise content • Classification of the notification (passive or active). In this case it is active • List the notification again under the Alert Tab/Notification Center or Privacy Settings. • Notification window in the middle of the screen

	• Specifying exactly if the PHI was accessed, copied, stolen or modified • Keeping a record of previous breaches and plans to avoid similar future breaches	
UI design requirements	The design should include the following: • A pop-up window that is classified based on color-coding. A red one always pops up automatically while yellow and green show a badge in Alerts tab or Message Center. • The pop-up window blurs or grays all user interface elements behind • The official logos of custodian and company hosting the information should be located in the top right next to the title • Alerts tab, notification center, and notification settings • Hazard icon next to the title (Privacy Breach Notification) • General notification • Technological suggestions should be taken by end-user such as changing the password, copying or downloading the records. • “OK” button to close the window • General title of the privacy breach in the home page before logging in the system bordered in red • A general advice on changing the password of other websites that the end-user is using the same email and password as part of the recovery plan • In case the investigation is not complete, a summary notification followed by either a series of notifications for updates or redirection to the Notification Center	
Privacy Patterns	Notification Privacy Pattern (4)	
Before and after task flows	**After**	
	Limiting Disclosure tasks	
Mapping to ISO 29100 Privacy Principles	**Principle ID**	**Privacy Principle**
	5	Use, retention and disclosure limitation
	7	Openness, transparency and notice
	9	Accountability
Verification by privacy professional	• Avoid generic designs • Avoid legal language • Insure that notifying the end-user should be after confirming the privacy breach not in case of a potential privacy breach • If the information regarding the breach is not complete, sentence clarifying the state should be included • Who is committed the breach usually is not included in the first notification because the investigation is still in progress as Privacy Professional ID 17 commented. • Privacy Professional ID 26 suggested an initial notification with basic information and a follow-up notification indicating	

	more information • "You have the right to file a complaint to the privacy commissioner office as part of the message" Privacy Professional ID 26 declared is an important aspect of the design • The privacy professionals ID 17 and 26 confirmed all aspects discussed in the workshops and listed above. The points that the privacy professional did not agree upon were removed or labelled by not verified in case it is a good design idea and participants discussed the aspect deeply
Challenges	• Covering all the legal, design and UI requirements without making it overwhelming to the end-user is a challenge
Additional Consideration	• In each organization, there should be a person who is assigned to be contacted when a breach occurs. This person should be trained and have a strong background on both NSPHIA legislation and the custodian privacy policy • *"*A custodian shall create and maintain a record of every security breach of the custodian's electronic information system that the custodian determines on a reasonable basis is likely to pose a risk to an individual's personal health information. (NSPHIA regulation section 10 (3))

2. Notification- Authorized Collection Notification	
Privacy Right	"The purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information." p 8. "The custodian may choose to obtain the individual's consent for the disclosure or give notice to the individual of the disclosure (section 10(2)(c))."
Reference to NSPHIA	• Section 24-29 of NSPHIA for collection, use and disclosure • Section 52-60 of NSPHIA for research purposes
Legal requirements	There are individuals who can access the PHI without a notification under NSPHIA including: • Individuals involved in your care and treatment, including students • Individuals who require the information to get payment for your health care • Anyone who can legally act for you with your consent • Specified organizations who have a legal right to see the information
	A notification should be sent to the end-user in the following cases: • In case of defining the purposes for collecting the PHI • A secondary use of PHI form the circle of care • For research purposes "The Personal Health Information Act

<table>
<tr><td></td><td colspan="3">(NSPHIA) allows for the use and disclosure of personal health information for research purposes, but places strict guidelines on the release of this information” Template 7-3 Data Disclosure Agreement Template</td></tr>
<tr><td><b>Privacy requirement</b></td><td colspan="3">• Patient consents
• Clear purposes
• What types of the PHI is going to be used</td></tr>
<tr><td><b>Design requirements</b></td><td colspan="3">• Considering a low number of notifications due to its low-risk classification
• Concise content
• The classification of the notification (passive or active). In this case, it is passive.
• The title should not indicate risk
• Updates if the collection purposes or the period for retention change
• Straightforward and unified platform
• Supporting a drop-down menu that lists all purposes for all the agents who can access or collect information</td></tr>
<tr><td><b>UI design requirements</b></td><td colspan="3">• Pop-up window and classified based on color-coding, which include yellow or green color because it is authorized access.
• Alerts tab, Notification Center, and Privacy Settings</td></tr>
<tr><td><b>Privacy Patterns</b></td><td colspan="3">Access Pattern (1)
Limiting Disclosure (3)
Notification Privacy Pattern (4)</td></tr>
<tr><td rowspan="2"><b>Before and after task flows</b></td><td colspan="2"><b>Before</b></td><td><b>After</b></td></tr>
<tr><td colspan="2">• Gaining patients’ consents</td><td>• Review the activity record
• Limit the disclosure</td></tr>
<tr><td rowspan="4"><b>Mapping to ISO 29100 Privacy Principles</b></td><td><b>Principle ID</b></td><td colspan="2"><b>Privacy Principle</b></td></tr>
<tr><td>2</td><td colspan="2">Purpose legitimacy and Collection limitation</td></tr>
<tr><td>5</td><td colspan="2">Use, retention and disclosure limitation</td></tr>
<tr><td>7</td><td colspan="2">Openness, transparency and notice</td></tr>
<tr><td><b>Verification by privacy professional</b></td><td colspan="3">The privacy professionals ID 17 and 26 confirmed all aspects discussed in the workshops and listed above. The points that the privacy professional did not agree upon were removed or labeled by not verified in case it is a good design idea and participants discussed the aspect deeply.</td></tr>
<tr><td><b>Challenges</b></td><td colspan="3">Further research should be conducted to identify detailed case scenarios based scenarios identified from a field study of
• When the notification is mandatory
• When it is not needed
• Cases that we can be avoided to reduce the number of notifications</td></tr>
<tr><td><b>Additional Consideration</b></td><td colspan="3">• “Collect, in relation to personal health information, means to gather, acquire, receive, gain access to or obtain the information</td></tr>
</table>

	by any means from any source" (NSPHIA, 2013)

3.1 Limiting Disclosure- Limit Who Can Access	
Privacy Right	• "Individuals have the right to request a record of activities in the form of a list of health agents or providers who accessed the online records and to minimize access to the information. Therefore, the individual has the right to access the information, have a list of who accesses the information, and to limit the individuals who can access the information and/or request not to disclose to certain information" (NSPHIA, 2015). • "You have the right to request that some or all of your personal health information not be collected, used or disclosed to specific individuals or organizations involved in your care" (Template 3-2 Notice of Purposes, NSPHIA 2013) • "You have the right to request that your personal health information not be used or disclosed by a specific health professional or organization." (Template 3-4 Written Privacy Statement, NSPHIA, 2013)
Reference to NSPHIA	• Sections 24 and 25 • Section 36
Legal requirements	When it applies: • If the patient used to allow information sharing but wants to stop • Want to define a list that can share and get access to the PHI • Limit the agents who can gain access (block access to some) • Block all
Privacy requirement	• In subsection 63(3) of the *Act*, a "*record of user activity related to an individual's personal health information*" means a report produced at the request of an individual for a list of users who accessed the individual's personal health information on an electronic information system for a time period specified by the individual. (*NSPHIA* regulation section 11(1))." • 'More explanation link' for consequences regarding choosing to hide or block some of the information.
Design requirements	Building on the design of the activity record page in a variety of ways as follows: • Group the agents based on their roles and then assign a level of access by a drop-down menu (define, limit, block). • Based on the medical document by adding another level of access. • Identifying the type of information that should be assigned access to, limit or block. • Based on the profiles as a predefined list of agents and their profiles. • White and blacklists: white for the pre-defined list and limiting the PHI disclosure; the blacklists to block agents from further

<table>
<tr><td></td><td colspan="2">access, collection, and sharing of PHI.</td></tr>
<tr><td><b>UI design requirements</b></td><td colspan="2">• Checkboxes beside each agent and type of medical document
• Drop down menu for assigning the level of access next to the agents
• Drop-down menus to assign levels of access next to each agent or medical record
• A matrix that has both the agent role and the type of the PHI</td></tr>
<tr><td><b>Privacy Patterns</b></td><td colspan="2">Limiting Disclosure (3)
Notification Privacy Pattern (4)</td></tr>
<tr><td rowspan="2"><b>Before and after Task flows</b></td><td><b>Before</b></td><td><b>After</b></td></tr>
<tr><td>• Notification of data collection has started
• Reviewing the activity record</td><td>• Notification of changes
• Reviewing privacy policy</td></tr>
<tr><td rowspan="2"><b>Mapping to ISO 29100 Privacy Principles</b></td><td><b>Principle ID</b></td><td><b>Privacy Principle</b></td></tr>
<tr><td>1
2
5
8</td><td>Consent and Choice
Purpose Legitimacy and Specification
Use, retention and disclosure limitation
Individual participation and access</td></tr>
<tr><td><b>Verification by privacy professional</b></td><td colspan="2">• The privacy professional ID 26 approved the concept of building on the design of the activity record.
• The privacy professionals ID 17 and 26 confirmed all aspects discussed in the workshops and listed above. The points that the privacy professional did not agree upon were removed or labelled by not verified in case it is a good design idea and participants discussed the aspect deeply.</td></tr>
<tr><td><b>Challenges</b></td><td colspan="2">• Trying to balance between viewing the activity records and adjusting the privacy settings on the activity record at the same time in one page.
• Separating the process into two pages would make the design less busy (study participants). Further research with particular patients would finalize the design.
• Two exceptions to not being able to limit, if the PHI is required by law (NSPHIA, 2013) and in emergency situations (interview study- Chapter 5)</td></tr>
<tr><td><b>Additional Consideration</b></td><td colspan="2">• Example scenario includes: “Helen has been receiving services from a psychologist for the several months. Initially, she was comfortable having the report be sent to her family physician. However, she now wants to keep information private. Under NSPHIA, she can request that the psychologist no longer send the reports to her family physician. The psychologist does not have to request the return of the previous reports, but must take reasonable steps to comply with Helen’s request.”
• In current practice, activity records are part of the EMR system</td></tr>
</table>

	that are still end-users ‘patients’ cannot get access to their PHI directly. To be able to review the activity record, a written request is submitted to the health care provider who would print a spreadsheet that contains 4 to 5 aspects: who, role, time, and the type of information was accessed. • By connecting the EMR to the online portal, not only patients can get access to their health records, which are part of their rights under NSPHIA, but also can have a level of control over their PHI. They can adjust the settings by providing them with details features to the activity record.

4. Consent to Collect PHI	
Privacy Right	• “An individual may request to limit or revoke consent for the collection, use or disclosure of personal health information in the custody or control of a custodian by giving notice to the custodian (section 17(1)).” • “A custodian may only collect, use or disclose personal health information if the individual consents and if it is reasonably necessary for a lawful purpose” (Chapter 5: Collection, Use and Disclosure, 2013).
Reference to NSPHIA	Section 17 Sections 24-29
Legal requirements	“The custodian must inform the individual of the consequences of limiting or revoking consent (section 17(4)),”
	Obtaining consent is in four main forms: • Patient wants to review the custodian’s privacy policy • Agreement to collect PHI • Agreement to third parties • The ability to opt in and out from agreements under NSPHIA.
Privacy requirement	• List of consequences in case of refusing to agree on the e-consents • Type of information that is going to collect • The purposes to collect the PHI • A basic consent to be able to use the online portal is the first step, and another consent is provided to the end-users right after they log in for more details on the aspects of the agreement (was not validated by the two privacy professionals)
Design requirements	• Having ‘Agreements Center’ or ‘Consent Center’ under ‘Privacy Settings’ tab that lists all types of agreements that have been signed by the end-user. • Designing an informed e-consent by including: bulletin points, checkboxes, and a second confirmation, languages options and audio sound of the agreement • Type of information that is being collected • Timestamp to be able to review agreements under settings

	• Short and concise consents • Duration of collection • How information is going to be disposed • One ‘Agree’ button • ‘Print Agreement’ button • Send a copy to email or by the regular mail and list the agreement in ‘Consents Collection’ tab under Privacy Settings • Informing the end-users that they can change their settings (in case they want to opt out) should be provided in the design of the online consent.
UI design requirements	• Consent to collect PHI after registration for the first time regarding agreement on the privacy policy • Changes on previous agreements require new consents and the new sections should be highlighted. • Structured based on sections that can expand for more details which includes a plus sign ✚ next to the section title that can expand for more details • A checkbox next to the heading or the title and under sections for details and ‘Check All’ button where applicable. • Live chat or real time communication before giving consents if the end-user needs clarifications • “Review Privacy Settings” or “Review the Consent” in case end-users decide to opt-out • “Manage Consents” icons in the homepage dashboard. • Links for ‘More Information’ • Link to the custodians’ privacy policy
Privacy Patterns	Access Pattern (1) Correction pattern (2) Limiting Disclosure (3) Notification Privacy Pattern (4)
Before and after Task flows	**Before** • Collecting information • Privacy policy notices **After** • Notification of agreement • Notification of changes in the consents
Mapping to ISO 29100 Privacy Principles	**Principle ID** — **Privacy Principle** 1 — Consent and Choice 2 — Purpose legitimacy and specification
Verification by privacy professional	• It is important to identify different types of scenarios to collect patient’s information: at registration to provide an online service, at limiting who can access the information and to share information to provide different types of medical services. • The privacy professionals ID 17 and 26 confirmed all aspects discussed in the workshops and listed above. The points that the

	privacy professional did not agree upon were removed or labeled by not verified in case it is a good design idea and participants discussed the aspect deeply.
Challenges	• Real-life scenarios that relates to health conditions would help participants design a consent that fit the potential end-user groups. This point is part of the future work. • How to encourage end-users read all aspects of the design to increase their level of understanding of the content
Additional Consideration	• One exception is “the revocation of consent does not apply to collection, use and disclosure of personal health information that a custodian is required by law to collect, use or disclose (section 17(6)).” • “Express consent is required for collection of personal health information for the purposes of fund-raising activities, market research, or marketing any service for a commercial purpose (section 32).” • All EMRs, EHRs, and healthcare systems are using servers in Canada. In case custodians use ‘outsourcing’ by storing the PHI outside Canada, the law requires an agreement and pre-requests qualifications to be fulfilled.

4.1 Notification After Providing Consents	
Privacy Right	“A notice of purposes is a notice or poster describing the purpose of the custodian’s collection, use and disclosure of personal health information (section 15)”
Reference to NSPHIA	Section 15 Template 3-2
Legal requirements	A notice of purposes must provide enough information for the individual to understand (NSPHIA, 2013): • Why their personal health information is being collected; • How it will be used; • Why it would be disclosed; • The individual’s rights under the Act; • Where the individual can obtain more information about the Act; and • How the individual can make a complaint or ask for a review under the Act
	A general statement about how the information will be used and disclosed (NSPHIA, 2013): • To provide the individual with health care • To communicate with or consult with other providers about the individual’s health care • To communicate with students in training with the custodian to support the individual’s health care

	• To obtain payment for the individual's health care, including payment through the Medical Services Insurance Program administered by Medavie Blue Cross, and payment from the individual's private insurance
Privacy requirement	• Send the notification when the collection process starts as a reminder. ▪ The notification should include: ▪ Who is doing the collecting ▪ What type of information specifying the duration of the collection process ▪ How the information is going to be used
Design requirements	• Considered as not a high-risk notification • Title of notification that does not indicate danger and the content should be simple and straightforward • A copy of the notification content is sent to the email
UI design requirements	• Color-coding is yellow or green indicating low-risk • A tab called 'Notification Center' • The notification should be in a form of a pop-up window and listed in the 'Notification Center' as well. • The notifications in the 'Notifications Center' are organized by dates and have checkboxes that indicate read or unread. • Q&A page that lists details on who can access for defined purposes and common questions regarding the notification. • 'OK' or 'Close' buttons on the notification pop-up window
Privacy Patterns	Access Pattern (1) Limiting Disclosure (3) Notification Privacy Pattern (4)
Before and after Task flows	**Before** • Consent to collect information **After** • Limiting access task • Reviewing activity record
Mapping to ISO 29100 Privacy Principles	**Principle ID** — **Privacy Principle** 6 — Accuracy and quality 7 — Openness, transparency and notice 8 — Individual participation and access
Verification by privacy professional	The Privacy Professional ID 17 suggests: • Avoid Alert icon ⚠ in low risk notifications • Avoid legal language such as the word 'collected' and encourage the use of 'shared' • The privacy professionals ID 17 and 26 confirmed all aspects discussed in the workshops and listed above. The points that the privacy professional did not agree upon were removed or labelled by not verified in case it is a good design idea and participants discussed the aspect deeply.
Challenges	• Balancing between notifying end-users and reducing the number of notifications to avoid the level of interruptions is a challenge.

Additional Consideration	• A notice of purposes should be placed in a location where an individual would easily be able to locate and read it (Chapter 3: Duties of a Custodian in NSPHIA, 2013) • It is essential to consider the period in which the custodian is going to retain and dispose of the PHI and send a notification when the collection process ends.

<table>
<tr><th colspan="3">5. Access, Add and Correct PHI</th></tr>
<tr><td><b>Privacy Right</b></td><td colspan="2">• “An individual has the right to access a record of personal health information about him/herself that is in the custody or under the control of a custodian (section 71).”
• “Individuals may request that the custodian correct information contained within their records of personal health information (section 85)”</td></tr>
<tr><td><b>Reference to NSPHIA</b></td><td colspan="2">• Sections 71-74
• Section 85
• Chapter 6 and 7</td></tr>
<tr><td rowspan="2"><b>Legal requirements</b></td><td colspan="2">There are individuals who can access the PHI without a notification under NSPHIA including:
• Individuals involved in your care and treatment, including students
• Individuals who require the information to get payment for your health care
• Anyone who can legally act for you with your consent
Specified organizations who have a legal right to see the information</td></tr>
<tr><td colspan="2">• The individual does not have to provide the reasons or purposes for which they are requesting the information (section 78).
• Including the patients’ rights in the online portal to access and correct information.</td></tr>
<tr><td><b>Privacy requirement</b></td><td colspan="2">• Regarding making corrections, it is a privacy right as well, but it has to be approved by the family physician to be able to upload the corrections to the online portal.
• Regarding deleting, medical information cannot delete a professional opinion about you, so it is going to be almost read-only when it comes to input from a physician.
• Restricted types of uploaded documents.</td></tr>
<tr><td><b>Design requirements</b></td><td colspan="2">• Marking the information added by users in colors
• New information added by end0users should be noted that it is uploaded by user.</td></tr>
<tr><td><b>UI design requirements</b></td><td colspan="2">• Text boxes to add information
• ‘Upload’ button</td></tr>
<tr><td><b>Privacy Patterns</b></td><td colspan="2">Access Pattern (1)
Correction Pattern (2)</td></tr>
<tr><td><b>Before and</b></td><td><b>Before</b></td><td><b>After</b></td></tr>
</table>

after Task flows	• Medical administrator links the EMR record to the online portal	• Notification of changes • Printing documents • Download documents
Mapping to ISO 29100 Privacy Principles	**Principle ID**	**Privacy Principle**
	6	Accuracy and quality
	7	Openness, transparency and notice
	8	Individual participation and access
Verification by privacy professional	• The privacy professionals ID 17 and ID 26 from DM workshops approved that accessing and correcting are fundamental aspects under NSPHIA individual's rights and the design requirements are both discussed by study participants and included in NSPHIA. • Some aspects are listed from the interview study Phase 2 in Chapter 5.	
Challenges	• Challenges are in current practices because NSPHIA requests to access and correct are made through paper work. • Another challenge is that EHRs in hospitals and EMRs in family physicians are still not linked in current practice.	
Additional Consideration	• One exception is to deny access to part of the PHI if the "access could result in a risk of serious harm to the treatment or recovery of the individual or to the mental or physical health of the individual" Chapter 6- NSPHIA, 2013. • Where a custodian refuses an individual's request for access in whole or in part, the custodian shall provide the individual with written notice setting out the reasons for the refusal and that the individual is entitled to make a complaint to the Review Officer (section 81(2)).	

7 Chapter 7: Contributions

We research contributions are summarized in the following sections.

7.1 Participatory Design Research in Technology Development (Hybridity)

7.1.1 Hybrid realm

We have focused on participatory practices that fall in the hybrid realm between the three domains explained in the research problem.

Our research area would expand the borders of PD research to create a third space (Muller and Druin, 2002), as mentioned in our Problem Definition section and in how Andersen et al. (2015) noted the need to expand its borders to new domains and new technologies. Working on this hybrid realm expands the borders of PD practices applications.

Participatory Design supports the concept of end-users' participation in the design lifecycle. However, we found that end-user participation was limited to having a group of users in one PD session. We believe that having multidisciplinary teams would expand the benefits of end-user participation and expand the borders of Participatory Design research in which it reveals valuable feedback from different stakeholders who are influenced directly or indirectly by the technology.

7.2 Shedding the Lights on New Research Areas

We focus on bringing diverse perspectives to construct usability and privacy-preserving collaboratively agreed-upon designs, which uncover new research fields to test in other contexts.

We believe that our research shows strength regarding the research gap and our research context as highlighted by CHI18 reviewers (who are privacy experts). Specifically, these reviewers agreed with the authors that it is essential to better integrate privacy law into the design and interaction aspects of private communication in medical settings. As Reviewer 2 eloquently points out, this work "moves beyond shallow interface concerns to a more holistic view of the issues limiting privacy legislation compliance." I strongly concur with Reviewer 2's excitement about the idea. Moreover, all reviewers enjoyed the combination of perspectives from different stakeholders as an important contribution to online privacy.

Continue working on the refining the framework by evaluating its effectiveness and focusing on adding elements to it such as the security patterns, would shed the lights on research areas that cover security and end-users participation.

7.3 Relating to a Real Case

Another important point is that we worked on a real case. We provide analysis of NSPHIA from a technological point of view and attempt to understand how practices are performed in relation to protecting patients' PHI. We believe it help other researchers in Nova Scotia understand the process, while inspiring researchers from other provinces to apply and compare the findings. There is not only a clear need for research that provides designers with a checklist to show compliance, but there is also a need to incorporate these laws and bridge the gap between policy and practice (Essén et al., 2017; Parks et al., 2011), especially between healthcare systems and government legislation (Wu et al., 2012). Bodker and Buur (2002) reiterated how important it is to support the "many-voiced nature of design".

We conducted the in-depth interviews to understand current practices and what we should implement to match the new proposed ideas with a real case. The preparation of the study and the interview questions helped us by revealing some challenges in understanding the flow of Personal Health Information in Nova Scotia. These challenges can help other researchers by either expanding the research or find ways to overcome them. We analyzed the list of recommended EMRs by provincial law, currently used EHR and the patient portal, which helped us focus on the provincial context and increased the chance of applying our framework in the real world as a real case. The review that we have done can help other researchers in the provinces who want to have a clear understanding of current healthcare systems and how they are connected.

By following our proposed methodology, we believe that we can add to the literature and bridge this gap in research and practice.

7.4 Theoretical Application Contribution

Applying both Grounded Theory and Activity Theory in a combined analytical framework add to the literature and bridge the theoretical application in HCI research for two reasons.

First, "Activity Theory has a tremendous capacity for growth and change" (Nardi, 1996, p. 5). It is used in HCI as a theory to offer a set of aspects of human activity and a set of concepts to describe the activity. We plan to expand its uses from formulating theories regarding human activities to applying it as an analytical approach to describe how people carry out activities and which element(s) of the theory they focus on during that activity.

A second way in which our research will add to the literature is that it will help determine the following: how teams with multidisciplinary backgrounds interact; what challenges such teams face and how they overcome them; which trade-offs they consider; how they create common agreed-upon designs; how they move toward the goal of the sessions and tasks; how they share experiences and expertise; and how they come up with a shared language. Therefore, our contribution will focus on integrating AT in PD as an analytical framework to understand how multidisciplinary teams interact in specific situations.

The usage and blending of theories such as Grounded Theory in HCI is rapidly expanding (Muller & Kogan, 2010). We have applied GT as an analytical framework for the requirement-gathering phase. In the literature, this framework is used to develop theories regarding end-users' behaviours (Muller & Kogan, 2010; Hekler et al., 2013). We believe that we can bridge the theoretical gap in HCI research (Nardi, 1997; Muller & Kogan, 2010; Hekler et al., 2013) by expanding the use borders of GT through formulating theory regarding end-users' behaviors to GT as an analytical approach to developing design guidelines.

7.5 Design and Visualization

The results from the cooperative prototyping sessions add to the literature and open a new research area for further testing. These design ideas are collaboratively agreed-upon designs by multidisciplinary stakeholders. Therefore, the input to these designs is not only from one perspective but several different perspectives. We cover a mix of usability, privacy preservation, Privacy-by-Design, and end-users' participation as designed by the proposed methodology. We will focus on explaining the challenges of applying these designs in the proof-of-concept phase, which will help designers to explore similar cases.

7.6 Usable Privacy-Preserving Framework

We developed a taxonomy of a usable privacy framework based on privacy from a legal perspective that is provided to privacy designers who have no or only limited knowledge in privacy from a legal perspective as shown in Section 6.6. Technology applications in eHealth should show compliance with privacy legislation where the flow of information in healthcare context is complicated (Fadlalla & Wickramasinghe, 2004) which adds to the need for effectives measures and frameworks to help designers show compliance.

We agree with Wu et al. (2012) that there is a need for effective measures to address the gap between the privacy legislation and healthcare systems. Moreover, “a single technology alone cannot meet all the privacy requirements to achieve PIPEDA compliance” in Canada (Szeto and Miri, 2007, p. 4). In our thesis, we take the first step toward developing effective measures to address the gap by building a usable privacy-preserving framework step by step, constructing the design ideas from different stakeholders while building our thesis.

We believe that our framework represents a contribution that can be applied to any privacy regulation to show compliance, which designers can integrate into the early design phase. The framework cover privacy rights, reference to NSPHIA sections, privacy design requirements, design requirements, User Interface elements, privacy patterns from reach phase 1, tasks that are associated with the requirements, mapping to ISO framework 29100, validation by privacy professionals, and additional considerations acting as a checklist for designers. We believe that the process of PD research forms an all-encompassing solution for privacy designers. Therefore, our contribution is both the privacy-preserving framework and the research methodology we followed during the construction of the framework.

7.6.1 Framework validation

Our proposed privacy-preserving framework will receive a formal evaluation method as we suggested in the future work by conducting a Hackathon where IT designers would use an extended version of framework supported with more details on tasks and tasks flows. However, to date each element of the privacy-preserving framework has been validated in its research phase. The proposed privacy patterns were validated by mapping them to international standards. These proposed patterns were refined to cover privacy principles that were not mapped. As an output from Phase 1, the patterns uncovered research gaps and helped in forming research questions and interview questions guide. The output of Phase 2 is design guidelines that acted as input to the next phase for refinements, which is Phase 3. The output of Phase 3 is refined design guidelines forming synthesized results from all previous phases, which act as minor validations as we move to the final phase in our research approach as our proposed privacy-preserving framework. The limitations we faced seemed primarily due to the lack of interest of the participants from different stakeholder groups (such as Physician Offices' Administrators) whose participation we expected would help to refine our design guidelines in the cooperative prototyping to address the administration perspective and PHIA representatives in the interview study to build a solid background of our understanding of the act privacy rules.

7.7 Reflection on our research methodology

We applied the methodologies of Participatory Design because of the way the research approach fit our context that requires multidisciplinary participation to be able to cover different aspects of designs and gain different feedback from different stakeholders. The research approach can be generalized to include contexts that need multidisciplinary participation. Conducting in-depth interviews in an early phase of design is an important aspect. This would form a guide to the next phases where most of the conflicts can be resolved at an early stage. Conducting CARD sessions to apply a high level of tasks analysis is beneficial because of its benefits in refining early requirements that usually reflect one perspective, which is the designer or the developer. Conducting more formal cooperative design techniques such as our proposed Decision-Making workshop would help solve the contradictions within the workshops by thinking about the conflict as a design problem that all participants can suggest solutions to overcome and be able to design collaboratively agreed upon designs that all participants are satisfied with. I believe this approach can be adopted by any other designers who are trying to show compliance with their privacy laws, either very specific one such as NSPHIA, or general ones such as the Canadian Data Protection Act (GDPA).

8 Chapter 8: Conclusion and Future Work

Looking at the history and the background of PD, we add to the literature as a contribution to the development of IT technologies that need a reasonable level of cooperation from multidisciplinary teams.

We have proposed privacy patterns to cover privacy rights based on NSPHIA as a case to represent privacy legislation. These patterns were used as an input to the analysis of the requirement-gathering phase in the form of in-depth interview study. A set of design guidelines was proposed and used to form the tasks of the cooperative prototyping sessions as a next research phase.

We developed a privacy-preserving framework based on legal perspective to construct collaborative agreed-upon designs by multidisciplinary teams acting as co-designers and co-evaluators.

8.1 Hackathon event

A formal way of testing is the next planned of this research. Conducting a hackathon event to evaluate the privacy-preserving framework that is based on legal perspective is an interesting way to validate the framework. A hackathon "(also known as a hack day, hackfest or codefest) is a design sprint-like event in which computer programmers and others involved in software development, including graphic designers, interface designers, project managers, and others, often including subject-matter-experts, collaborate intensively on software projects" (Leckart, 2012). Participants will be designing high fidelity prototypes and theses designs will go through an evaluation process that is divided into two parts: first evaluation is to evaluate the framework by evaluating the participants' understanding and ability to code the aspects of the framework. The second evaluation is going to be applied to the results from the first evaluation, which is the proposed designs in form of prototypes. These designs are going to be evaluated for their NSPHIA compliance.

We plan to design it to be a controlled study in a lab where participants, who are IT designers with different computer science backgrounds, are asked to perform some design tasks based on our framework. The prototypes are going to be validated by privacy professionals as a final evaluation at the end of the hackathon.

8.2 Expanding the research

Further research is anticipated after the iteration process ends. We suggest research directions such as cooperation of the personalization of the user interface design according to the end-users groups with our privacy-preserving designs. Also, piloting the collaborative agreed-upon designs in the MyHealthNS patient portal or similar portals to test patients' acceptance level.

I am planning to write a technical report that is not 100% technical aims to be provided to non-computer science majored individuals who might be interested in looking at the framework or a simplified version of the whole process with only the framework. This could benefit research teams who are working to improve MyHealthNS and individuals from the public. The Act is new, and MyHealthNS is still under testing; therefore, I believe the framework is considered to be a valuable contribution to this mixed research area of law, eHealth, and Participatory Design.

8.3 Cooperative Evaluation

"Cooperative evaluation" is a variant of thinking aloud, in which the user is encouraged to see himself as a collaborator in the evaluation rather than just a subject. As well as getting the user to think aloud, the evaluator will ask such questions as "Why? " and "What if…? ", and request clarification of responses (Wright & Monk, 1991). In this strategy, the user is encouraged to criticize the system rather than simply suffer it actively, and the evaluator can clarify points of confusion, thus maximizing the effectiveness of the approach.

We will be following a list of tasks aimed at: testing the proof-of-concept UI prototype; uncovering usability problems and suggesting ways to solve them; and combining user feedback with that from the cooperative prototyping session to form a synthesized list of design guidelines. The output will be added to the main potential contribution (i.e., the usable privacy-preserving framework), as the privacy checklist should be evaluated and prove its efficiency.

The cooperative evaluation session will be divided into three phases:

(1) Introduction and session objective, which will feature an Evaluation Frame poster hung on the wall. It will be used for the analysis process.

(2) A "think aloud" session that will have three to four teams conducted at the same time and include one to three participants along with an HCI specialist (designer) and a researcher. Each team will examine the proof-of-concept prototypes based on specified tasks. An observer will write down the dialog and user interaction, such as

the users' hypothesis, choices, impressions, and commentaries about the prototype. After completing this session, the teams will start discussing the next session.

(3) The Evaluation Frame session will highlight the results from the discussion, stating the good and bad characteristics of the prototype and developing a critique that outlines the recommendations to overcome the bad characteristics in the form of post-it notes on the poster.

Testing privacy is critical even if the end-users' main task is not privacy, as users will be accessing the online portal to explore their PHI. They will interact with privacy designs as they process other tasks, such as looking at their activity record or updates of their record.

We are planning to design a study that examines the privacy-preserving user interface collaboratively with end-users. We intend to design the tasks in such a way that privacy is a secondary task for the end-users to examine how accurately end-users are going to deal with the privacy notices and other aspects. This helps us explore how users might react and what next steps they might take, which will reveal design problems as well as indicate design considerations we should apply in refining the privacy-preserving UI. For example, we could design a task as if the end-user were going to look for the results of his/her latest visit to the family physician. While the user is browsing the record, a notification message could pop-up asking what it should include as common agreed-upon designs from the cooperative prototyping session. We will focus on the end-users' reactions to determine which design considerations should be applied to recover the usability issues.

Additionally, we will apply Activity Theory to explore how and when problems might be uncovered and what sequence users might follow in uncovering and recovering from privacy design problems. By apply AT, we aim at opening new research areas for testing end-users' behaviors when dealing with privacy issues in a user interface in the context of eHealth or healthcare applications. We plan to apply Whiteside et al.'s (1988) usability measures to cover the following:

- Commands used
- Repetitions of failed commands
- Runs of successes and failures
- Good and bad features recalled by users
- Available commands not invoked/regressive behaviors

- Users’ preference for the system
- Percentage of tasks completed in a period
- Counts or percentages of: errors and superior competitor products on a measure
- Ratios of successes to failures and favorable to unfavorable comments
- Time to complete a task spent on errors and spent using help or documentation
- Frequencies of:
    - Help and documentation use
    - Interfaces, misleading users
    - Users needing to work around a problem
    - Users disrupted from a work task
    - Users losing control of the system
    - Users expressing frustration or satisfaction

We plan to recruit a wide range of end-users and to explore their reactions and needs while applying the notion of PD. Potential participants include any member of the public who had at least one visit to the family physician and have a medical record. Future work could include focusing on each of these groups and studying their specific needs, from which a UI could be designed that is usable, privacy-preserving, and designed specifically to those groups.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2017). Nudges for privacy and security: understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 44.

Agency for Healthcare Research and Quality. (2017). Electronic Medical Record Systems. Retrieved on 10th May, 2017 from https://healthit.ahrq.gov/key-topics/electronic-medical-record-systems

Aljohani M., Hawkey K., and Blustein. J., (2016, July). Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 91-102). Springer International Publishing

Alshenqeeti, H. *(2014). Interviewing as a data collection method: A critical review. English Linguistics Research, 3 (1), 39-45. https://doi.org/10.5430/elr.v3n1p39*

Andersen*, L.* B., Danholt, P., Halskov, K., Hansen, N. B., & Lauritsen, P. *(2015). Participation as a matter of concern in participatory design. CoDesign, 11(3-4), 250-261.*

Anderson, C. and Agarwal, R. (2011) 'The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information', Information Systems Research, Vol. 22, No. 3, pp.469–490.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), 279-314.

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E. (2011). Personal health records: a scoping review. Journal of the American Medical Informatics Association. 18(4): 515-522.

Arnowitz, J., Arent, M., & Berger, N. (2010). *Effective prototyping for software makers*. Elsevier.

Assal, H., & Chiasson, S. (2018). Security in the software development lifecycle. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018) (pp. 281-296).

Balebako, R., & Cranor, L. (2014). Improving app privacy: Nudging app developers to protect user privacy. IEEE Security & Privacy, 12(4), 55-58.

Bardram, J. E. (1997). Plans as situated action: an activity theory approach to workflow systems. In *Proceedings of the Fifth European Conference on Computer Supported Cooperative Work* (pp. 17-32). Springer Netherlands.

Bergold, J., & Thomas, S. (2012). Participatory research methods: A methodological approach in motion. *Historical Social Research/Historische Sozialforschung*, 191-222.

Binder, T. Why Design: Labs? Design Inquiries 2007. Retrieved From: www.nordes.org,Stockholm (accessed 5 January, 2010)

Björgvinsson, E., Ehn, P., & Hillgren, P. A. (2010, November). Participatory design and democratizing innovation. In *Proceedings of the 11th Biennial participatory design conference* (pp. 41-50). ACM.

Bødker, K., Kensing, F., & Simonsen, J. (2009). *Participatory IT design: designing for business and workplace realities*. MIT press.

Bødker, S., & Grønbæk, K. (1991a). Cooperative prototyping: users and designers in mutual activity. *International Journal of Man-Machine Studies*, *34*(3), 453-478.

Bødker, S., & Grønbæk, K. (1991b). Design in action: From prototyping by demonstration to cooperative prototyping. In *Design at work: Cooperative design of computer systems*. Lawrence Erlbaum Associates, Incorporated.

Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input* (pp. 3-7). Watertown, MA: Pathfinder International.

Breaux, T., & Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. IEEE transactions on software engineering, 34(1), 5-20.

Brounéus, K. (2011). In-depth Interviewing, The process, skill and ethics of interviews in peace research. Höglund, Kristine & Magnus Öberg (eds), 130-145.

Buschmann, F., Henney, K., & Schimdt, D. (2007). Pattern-oriented Software Architecture: On Patterns and Pattern Language (Vol. 5). John wiley & sons.

Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., & Stal, M. (1996). A system of patterns: Pattern-oriented software architecture.

Buur, J., Binder, T., & Brandt, E. (2000, December). Taking video beyond 'hard data'in user centred design. In *Participatory design conference* (pp. 21-29).

Bygholm, A., & Kanstrup, A. M. (2017). This Is not Participatory Design–A Critical Analysis of Eight Living Laboratories. *Participatory Design & Health Information Technology*, *233*, 78.

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

Canada's Health Informatics Association. (2012). Privacy for patient portals: 2012 guidelines for the protection of health information. Retrieved from: http://www.ehealthontario.on.ca/images/uploads/pages/documents/Privacy-Security-for-Patient-Portals.pdf

Canadian Medical Protective Association. (2005). Using email communication with your patients: Legal risks. Retrieved https://www.cmpa-acpm.ca/-/using-email- communication-with-your-patients-legal-ris-1

Cataldi, S. (2018). A proposal for the analysis of the relational dimension in the interview techniques: a pilot study on in-depth interviews and focus groups. Quality & Quantity, 52(1), 295-312.

Cavoukian, A. (2013a). Privacy by Design: Leadership, Methods, and Results. In European Data Protection: Coming of Age (pp. 175-202). Springer Netherlands.

Cavoukian, A. (last access 2014b). 7 Foundational Principles: Privacy By Design: http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative research. Sage Publications Ltd, London.

Charmaz, K. (2014). Constructing grounded theory. Sage.

Chung, E. S., Hong, J. I., Lin, J., Prabaker, M. K., Landay, J. A., & Liu, A. L. (2004, August). Development and evaluation of emerging design patterns for ubiquitous computing. In Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques (pp. 233-242). ACM.

Clarke, R. (2009). Privacy impact assessment: Its origins and development. Computer law & security review, 25(2), 123-135.

Compagna, L., El Khoury, P., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artificial Intelligence and Law, 17(1), 1-30.

Coombes, L., Allen, D. Humphrey, D. H., & Neale, J. (2009). In-depth interviews. Research methods for health and social care, 197-210

Costabile, M. F., Fogli, D., Mussio, P., & Piccinno, A. (2006). End-user development: The software shaping workshop approach. In *End-user development* (pp. 183-205). Springer, Dordrecht.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J. on Telecomm. & High Tech. L., 10, 273.

Department of Family Practice. (2017). SHARE (Secure Health Access Record) – DFP. Retrieved on 10th May, 2017 from http://www.cdha.nshealth.ca/district-department-family-practice/practice-support/share-secure-health-access-record

Dingledine, R., Mathewson, N., and Syverson, P., "Tor: The Second-Generation Onion Router," In Proceedings of the 13th USENIX Security Symposium, 2004.

Doctors Nova Scotia. (2014). EMR benefits. Retrieved on 10th May, 2017 from http://www.doctorsns.com/en/home/practiceresources/electronic-medical-records/EMR-benefits.aspx

Druin, A., Bederson, B. B., Rose, A., & Weeks, A. (2009). From New Zealand to Mongolia: Co-designing and deploying a digital library for the world's children. *Children Youth and Environments*, *19*(1), 34-57.

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1065-1074). ACM.

Engeström, Yrjö. (1987) Learning by Expanding, An Activity-Theoretical Approach to Developmental Research , Orienta-Konsultit Oy, Helsinki, Finland.

Essén, A., Gerrits, R., & Kuhlmann, E. (2017). Patient accessible electronic health records: Connecting policy and provider action in the Netherlands. *Health Policy and Technology*.

Fadlalla, A., & Wickramasinghe, N. (2004). An integrative framework for HIPAA-compliant I* IQ healthcare information systems. *International Journal of Health Care Quality Assurance*, *17*(2), 65-74

Fischer-Hübner,S. Köffel C., Pettersson J., Wolkerstorfer, Holtz G., König U., Kellermann H., (2010) Prime Life. Retrieved from: http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf

Fliess, S., & Becker, U. (2006). Supplier integration—Controlling of co-development processes. *Industrial Marketing Management*, *35*(1), 28-44.

Grimshaw, P. & Burgess, T. 2014 The emergence of 'zygotics': using science fiction to examine the future of design prototyping. *Technological Forecasting and Social Change* 84, 5–14.

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. Information and Software Technology, 51(2), 337-350.477–564 (2006)

Guion, L. A., Diehl, D. C., & McDonald, D. (2001). *Conducting an in-depth interview*. University of Florida Cooperative Extension Service, Institute of Food and Agricultural Sciences, EDIS.

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. Computers, Privacy & Data Protection, 14(3).

Hafiz, M. (2006, October). A collection of privacy design patterns. In Proceedings of the 2006 conference on Pattern languages of programs (p. 7). ACM.

Health and Wellness. (2016). Federal and Provincial Governments Launch MyHealthNS to Improve Health Care in Nova Scotia. Retrieved From: https://novascotia.ca/news/release/?id=20160728004

Heart, T., Ben-Assuli, O., & Shabtai, I. (2017). A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy and Technology, 6(1), 20-25

Hekler, E. B., Klasnja, P., Froehlich, J. E., & Buman, M. P. (2013, April). Mind the theoretical gap: interpreting, using, and developing behavioral theory in HCI research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3307-3316). ACM.

Hodge, T., & Giokas., D. (2011). EMR, EHR, and PHR – Why All the Confusion?. *Canada Health Infoway.* Retrived From: https://www.infoway-inforoute.ca/en/what-we-do/blog/digital-health-records/6852-emr-ehr-and-phr-why-all-the-confusion.

Hoepman. J. (2014). June. Privacy design strategies. In *IFIP International Information Security Conference* (pp. 446-459). Springer, Berlin, Heidelberg

Hoffer, j., Joey G., Valacich, J., (2011). Modern Systems Analysis and Design, 6th edition, Prentice Hall.

ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27

Iwaskow, E. and Russell, M. (June, 2015). New Technology Meets New Legislation. Connecting Patients, Providers, and Health Information. Retrieved From: http://www.e-healthconference.com/pastpresentations/2015/20157981679/FINAL_eHealth_2015_05_29.pdf?AF=Download&AA=202,1452&AD=DlFile

Kanstrup, [A] A. M., Madsen, J., Nøhr, C., Bygholm, A., & Bertelsen, P. (2017). Developments in Participatory Design of Health Information Technology: A Review of PDC Publications from 1990–2016. *Participatory Design & Health Information Technology*, *233*, 1.

Kanstrup, [b] A. M., Bygholm, A., & Bertelsen, P. (Eds.). (2017). *Participatory Design & Health Information Technology* (Vol. 233). IOS Press.

Kensing, F., & Madsen, K. H. (1992). *Generating visions: Future workshops and metaphorical design* (pp. 155-168). L. Erlbaum Associates Inc.

Krishnaswamy, A. 2004. Participatory Research: Strategies and Tools. *Practitioner: Newsletter of the National Network of Forest Practitioners 22: 17-22*

Kuutti, K. (1996). Activity theory as a potential framework for human-computer interaction research. *Context and consciousness: Activity theory and human-computer interaction*, *17*.

Kuutti, Kari and Tuula Arvonen. (1992) "Identifying Potential CSCW Applications by Means of Activity Theory Concepts: A Case Example" Proceedings of the Conference on Computer Supported Cooperative Work (CSCW). New York, ACM Press, 233-240.

Latulipe, C., Gatto, A., Nguyen, H. T., Miller, D. P., Quandt, S. A., Bertoni, A. G., ... & Arcury, T. A. (2015, April). Design considerations for patient portal adoption by low-income, older adults. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 3859-3868). ACM.

Leckart, S., (March 2012). The Hackathon Is On: Pitching and Programming the Next Killer App.

Luger, E., Urquhart, L., Rodden, T., & Golembewski, M. (2015, April). Playing the legal card: Using ideation cards to raise data protection issues within the design process. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 457-466). ACM.

Macaulay, L. (1995). Cooperation in understanding user needs and requirements. Computer integrated manufacturing systems, 8(2), 155-165.

Mack, N., Woodsong, C., MacQueen, K. M., Quest, G., & Namey, E. (2011). Qualitative Research Methods: A Data Collector's Field Guide. North Carolina, USA: Family Health International (FHI).

Maguire, M., Kirakowski, J., & Vereker, N. (1998). RESPECT: User centred requirements handbook.

Mannonen, P., Aikala, M., Koskinen, H., & Savioja, P. (2014, December). Uncovering the user experience with critical experience interviews. In Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: the Future of Design (pp. 452-455). ACM.

McPhail, B., Costantino, T., Bruckmann, D., Barclay, R., & Clement, A. (1998). CAVEAT exemplar: Participatory design in a non-profit volunteer organisation. *Computer Supported Cooperative Work (CSCW)*, *7*(3-4), 223-241.

Milena, Z. R., Dainora, G., & Alin, S. (2008). Qualitative research methods: a comparison between focus-group and in-depth interview. *Annals of the University of Oradea, Economic Science Series*, *17*(4), 1279-1283.

Milewski, J., & Parra, H. (2011, May). Gathering requirements for a personal health management system. In CHI'11 Extended Abstracts on Human Factors in Computing Systems (pp. 2377-2382). ACM.

Miller Jr, D. P., Latulipe, C., Melius, K. A., Quandt, S. A., & Arcury, T. A. (2016). Primary care providers' views of patient portals: interview study of perceived benefits and consequences. Journal of medical Internet research, 18(1).

Mitchell, V., Ross, T., May, A., Sims, R., & Parker, C. (2016). Empirical investigation of the impact of using co-design methods when generating proposals for sustainable travel solutions. *CoDesign*, *12*(4), 205-220.

Moran.T., (2006). Activity: Analysis, Design, and Management. In: Bagnara, Sebastiano and Smith, Gillian Crampton (eds.). "Theories and Practice in Interaction Design (Human Factors and Ergonomics Series)". Lawrence Erlbaum Associate

Mørch, A. I., Engen, B. K., & Åsand, H. R. H. (2004, July). The workplace as a learning laboratory: The winding road to e-learning in a Norwegian service company. In Proceedings of the eighth conference on Participatory design: Artful integration: interweaving media, materials and practices-Volume 1 (pp. 142-151). ACM.

Muller, M (2015). PICTIVE -An Exploration in Participatory Design. ACM journal 14 (4): 225-232

Muller, M. J. & Druin, A. (2003). Participatory design: the third space in HCI. Human-computer interaction: Development process, 4235, 165-185.

Muller, M. J., & Kogan, S. (2010). Grounded theory method in HCI and CSCW. *Cambridge: IBM Center for Social Software*, 1-46.

Nardi, B. A. (1996). Activity theory and human-computer interaction. *Context and consciousness: Activity theory and human-computer interaction*, *436*, 7-16.

National Research Council. (2003). Who goes there? Authentication through the lens of privacy. Washington, D.C: National Academies Press.

Nightingale MD. (2017). On Demand ASP EMR. Retrieved on 10th May, 2017 from http://www.nightingalemd.ca/products-services-1/emr/

Nova Scotia Health Authority. (2017). SHARE Clinical Portal? Retrieved on 10th May, 2017 from http://www.nsnig.ca/doc_view/248-share-clinical-portal.html

NSPHIA. Chapter 1: Complying with NSPHIA. November 1st, 2013 Retrieved From: https://novascotia.ca/DHW/PHIA/documents/chapters/1-Complying-with-PHIA.pdf

OECD (1980). OECD guidelines on the protection of privacy and trans-border flows of personal data. http://www.oecd.org/home/

Office of the privacy commissioner of Canada (2014). Overview of privacy legislation in Canada. Retrieved From: https://www.priv.gc.ca/en/privacy-topics /privacy-laws-incanada/the-personal-information-protection-and-electronicdocuments-act-pipeda/

Oliver, I., On Finding Reasonable Measures To Bridge the Gap Between Privacy Engineers and Lawyers. Privacy Perspectives. (July 29, 2014). Accessed (August, 2016). Retrieved From: https://iapp.org/news/a/on-finding-reasonable-measures-to-bridge-the-gap-between-privacy-engineers-and-lawyers/

Olsson, E. (2004). What active users and designers contribute in the design process. *Interacting with computers*, *16*(2), 377-401.

Pai F-Y, Huang K-I. Applying the technology acceptance model to the introduction of healthcare information systems. Technological Forecasting and Social Change. 2011;78(4):650–660

Pallozzi-Ruhm, J. and Agee, R. Privacy Compliance in Digital Age. (May 2016). Retrieved From: https://www.slideshare.net/theSCCE/privacy-compliance-in-the-digital-age-61825564

Parks, R., Chu, C. H., & Xu, H. (2011). Healthcare information privacy research: Issues, gaps and what next?. In *AMCIS*.

Patton, M.Q. 1987. How to use qualitative methods in evaluation. London: Sage Publications.

Personal Health Information Act (NSPHIA), (2013) Accessed 2014, Department of health and Wellness, Retrieved From: http://novascotia.ca/dhw/phia/

Pilemalm, S., & Timpka, T. (2008). Third generation participatory design in health informatics—making user participation applicable to large-scale information system projects. *Journal of biomedical informatics*, *41*(2), 327-339.

Porekar, J., Jerman-Blazic, A., & Klobucar, T. (2008, February). Towards organizational privacy patterns. In Digital Society, 2008 Second International Conference on the (pp. 15-19). IEEE.

Practimax. (2017). Practimax EMR Features. Retrieved on 10th May, 2017 from http://practimax.ca/practimax-emr/features

Przybylo, J. A., Wang, A., Loftus, P., Evans, K. H., Chu, I., & Shieh, L. (2014). Smarter hospital communication: secure smartphone text messaging improves provider satisfaction and perception of efficacy, workflow. Journal of hospital medicine, 9(9), 573-578.

QHR Technologies. (2017). Accuro EMR - #1 Electronic Medical Record platform in Canada. Retrieved on 10th May, 2017 from http://www.qhrtechnologies.com/electronic-medical-records/accuro-product-suite/accuro-emr/

Ramakrishna, S., & Paschke, A. (2014). Bridging the gap between Legal Practitioners and Knowledge Engineers using semi-formal KR. arXiv preprint arXiv:1406.0079.

Reymen, I. M. M. J., Whyte, J. K., & Dorst, C. H. (2005, April). Users, designers and dilemmas of expertise. In *Proceedings of the International Conference on Inclusive Design (Include 2005)*(pp. 5-8).

Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F., & Friedman, B. (2006, October). Privacy patterns for online interactions. In Proceedings of the 2006 conference on Pattern languages of programs (p. 12). ACM.

Rothmann, M. J., Danbjørg, D. B., Jensen, C. M., & Clemensen, J. (2016, August). Participatory design in health care: participation, power and knowledge. In *Proceedings of the 14th Participatory Design Conference: Short Papers, Interactive Exhibitions, Workshops-Volume 2* (pp. 127-128). ACM.

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015, July). A design space for effective privacy notices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 1-17).

Serenko, N., & Fan, L. (2013). Patients' perceptions of privacy and their outcomes in healthcare. International Journal of Behavioral and Healthcare Research, 4(2), 101-122.

Solomon, J., Scherer, A. M., Exe, N. L., Witteman, H. O., Fagerlin, A., & Zikmund-Fisher, B. J. (2016, May). Is This Good or Bad?: Redesigning Visual Displays of Medical Test Results in Patient Portals to Provide Context and Meaning. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (pp. 2314-2320). ACM.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. Software Engineering, IEEE Transactions on, 35(1), 67-82.

Spinuzzi, C. 2005. The methodology of participatory design. *Technical communication*, *52*(2), pp.163-174.

Sun, S., Zhou, X., Denny, J. C., Rosenbloom, T. S., & Xu, H. (2013, April). Messaging to your doctors: understanding patient-provider communications via a portal system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1739-1748). ACM.

Swan, M. (2009) 'Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and qualified self-tracking', Environmental Research and Public Health, Vol. 6, No. 2, pp.492–525.

Swire. P., & Anton, A., Engineers and Lawyers in Privacy Protection: Can We All Just Get Along? Privacy Perspectives. (January 13, 2014). Accessed (August, 2016). Retrieved From: https://iapp.org/news/a/engineers-and-lawyers-in-privacy-protection-can-we-all-just-get-along/

Szeto, M., & Miri, A. (2007, July). Analysis of the use of privacy-enhancing technologies to achieve PIPEDA compliance in a B2C e-business model. In *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the* (pp. 6-6). IEEE.

Terry, Amanda L., Moira Stewart, Martin Fortin, Sabrina T. Wong, Maureen Kennedy, Fred Burge, Richard Birtwhistle, Inese Grava-Gubins, Greg Webster, and Amardeep Thind. (2014). Gaps in primary healthcare electronic medical record research and knowledge: findings of a pan-Canadian study. Healthcare Policy, 10(1), 46.

Tudor, L. G., Muller, M. J., Dayton, T., & Root, R. W. (1993, October). A participatory design technique for high-level task analysis, critique, and redesign: The CARD method. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 37, No. 4, pp. 295-299). Sage CA: Los Angeles, CA: SAGE Publications.

Turner, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. The Qualitative Report, 15 (3), 754-760. Agency for Healthcare Research and Quality. (2017). Electronic Medical Record Systems. Retrieved on 10th May, 2017 from https://healthit.ahrq.gov/key-topics/electronic-medical-record-systems

United States Agency for International Development's Center for Development Information and Evaluation. USAID (1996). Conducting Key Informant Interviews. (Performance Monitoring and Evaluation TIPS) Available at http://www.usaid.gov/pubs/usaid_eval/pdf_docs/pnabs541.pdf

Usability Evaluation Basics. Retrieved From: <URL:https://www.usability.gov/what-and-why/usability-evaluation.html>

Van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014). Designing privacy-by-design. In Privacy Technologies and Policy (pp. 55-72). Springer Berlin Heidelberg.

W3C, Platform for Privacy Preferences, P3P 1.0, 2002. URL: http://www.w3.org/P3P/

Waart, V., Mulder, I., & Bont, C., (2015, May). Participatory prototyping for future cities. In *4th Participatory Innovation Conference 2015* (p. 337).

Wallace Foundation. Knowledge Center. Workbook E-Indepth-Interviews. Accssed January 2017. Retrieved From: http://www.wallacefoundation.org/knowledge-center/Documents/Workbook-E-Indepth-Interviews.pdf

Weber, S., Harbach, M., & Smith, M. (2015). Participatory Design for Security-Related User Interfaces. *Proc. USEC*, *15*.

Wilson EV, Lankton NK. Modeling patients' acceptance of provider-delivered e-health. Journal of the American Medical Informatics Association. 2004;11(4):241–248.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006, April). Do security toolbars actually prevent phishing attacks?. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 601-610). ACM.

Wu, R., Ahn, G. J., & Hu, H. (2012, January). Towards HIPAA-compliant healthcare systems. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium* (pp. 593-602). ACM.

Yamauchi, Y. (2009, May). Power of peripheral designers: how users learn to design. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (p. 13). ACM.

Appendix A: The Privacy Patterns Diagrams

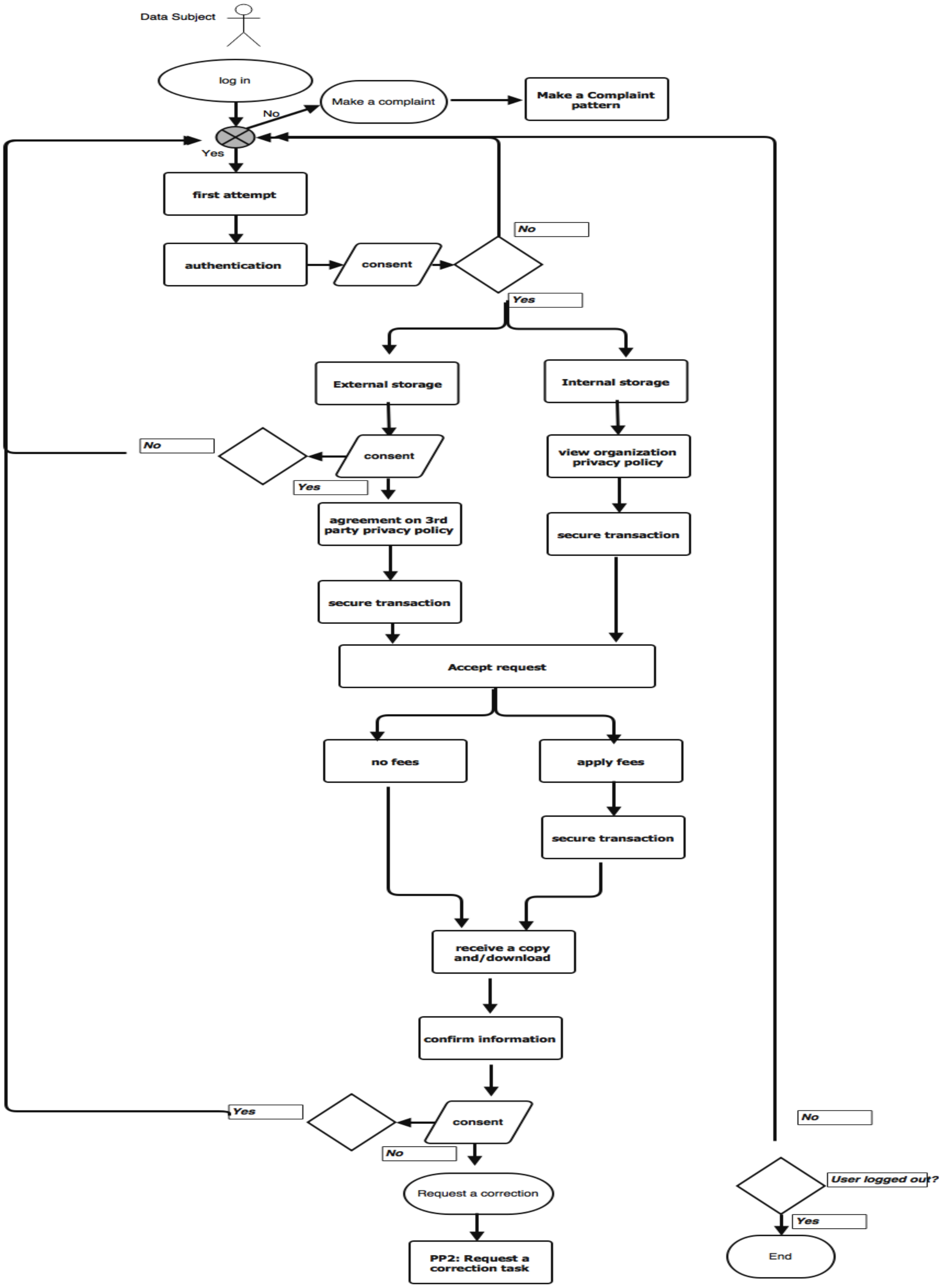


Figure 31. Access privacy pattern

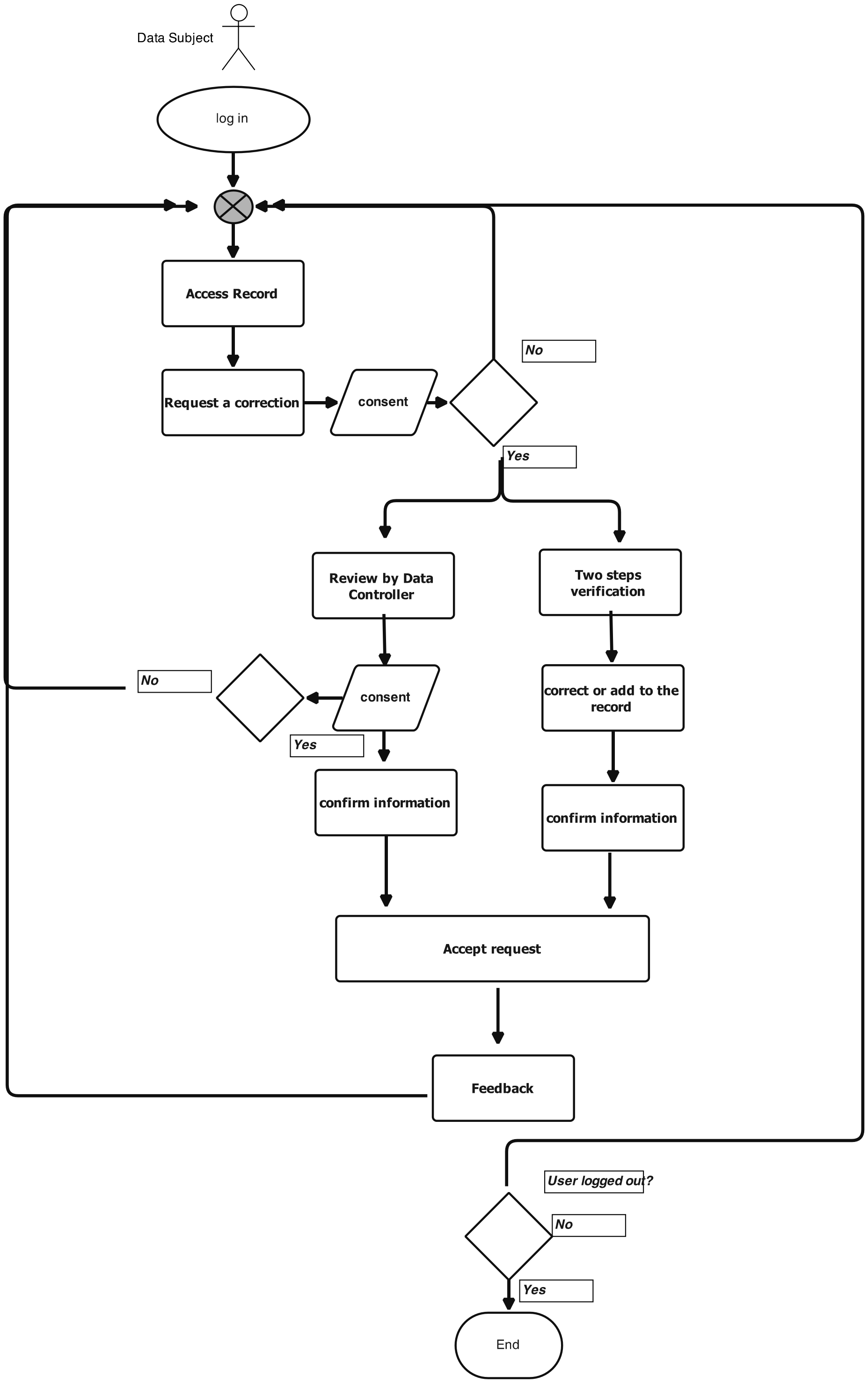


Figure 32. Correction privacy pattern

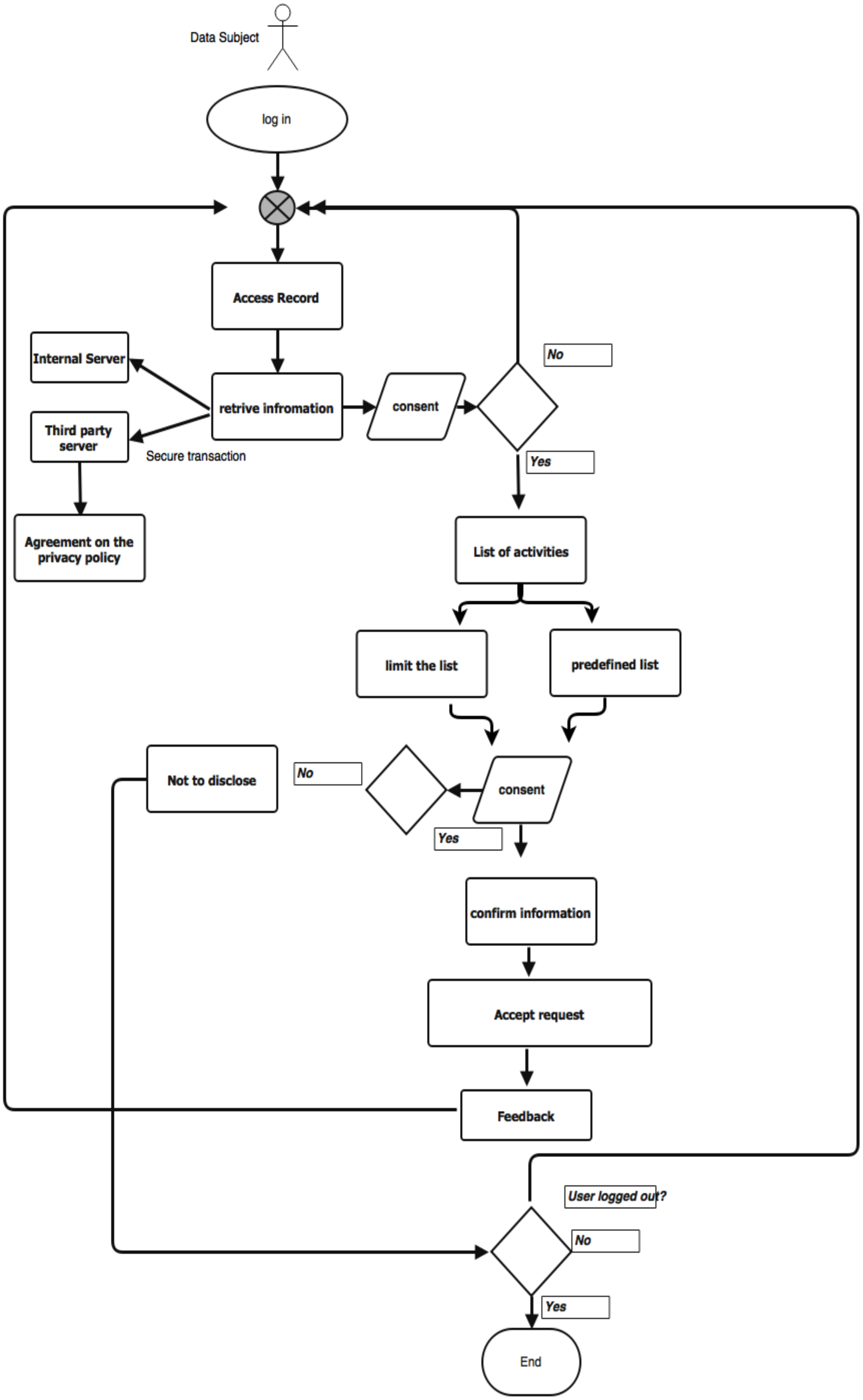


Figure 33. Limiting disclosure privacy pattern

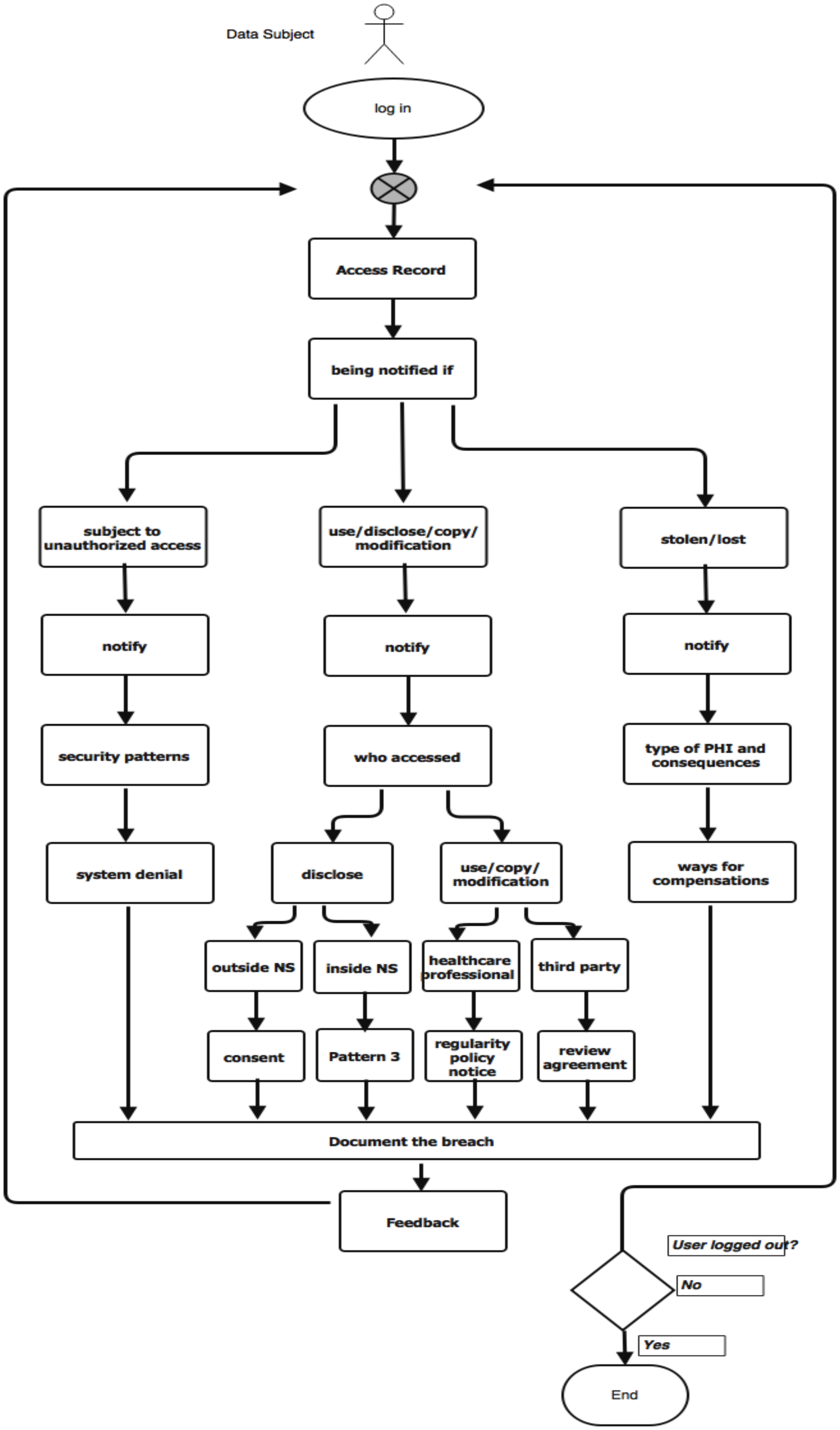


Figure 34. Notification privacy pattern

Appendix B: Code Categories of The Interview Study Analysis Process

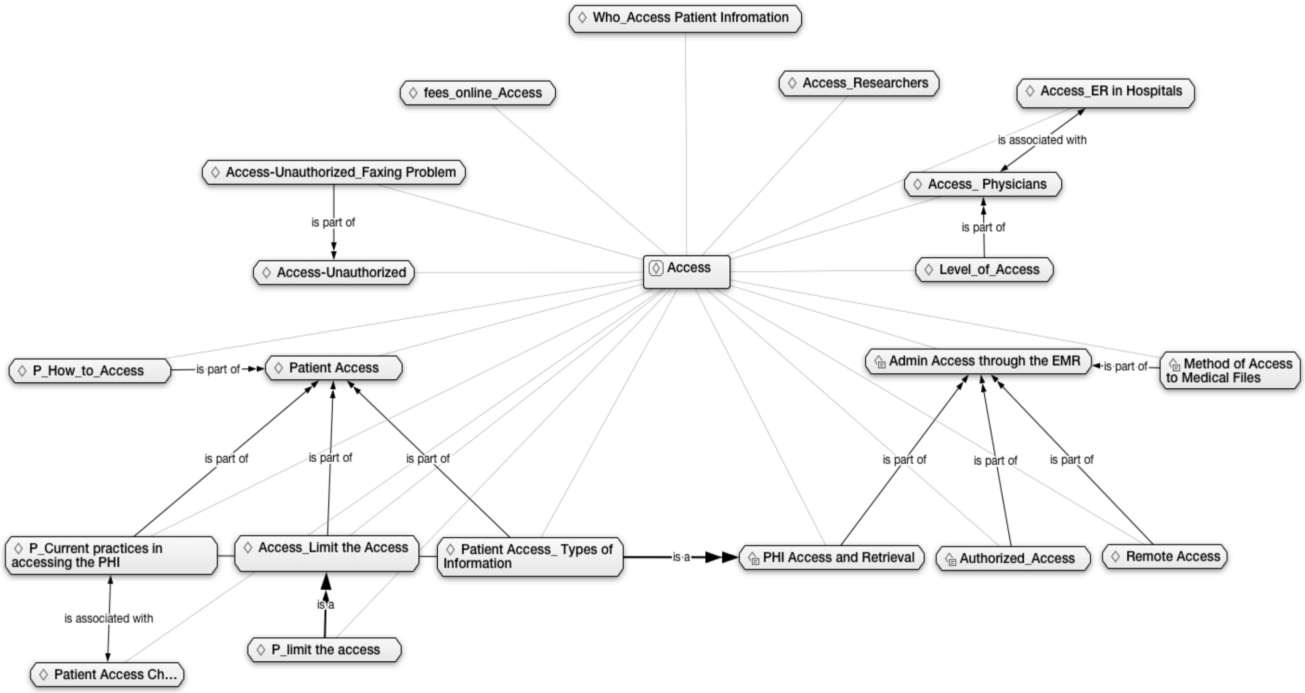


Figure 35. Access category

In the access category, we analyzed the collected qualitative data and we found that Access category includes 6 codes and 8 sub-codes. After removing reparations and combining codes that share the same meaning. Codes focus on current practices of patient access, admins access, unauthorized access, researchers and physicians access and who can access patient information. The access category can be considered as a category that is linked to almost all other categories through codes and/or sub-codes.

The second category is Electronic Medical Records and their architectures and how they are connected to online patient portals along with challenges is using them by doctors' office administrators as shown in Figure 36.

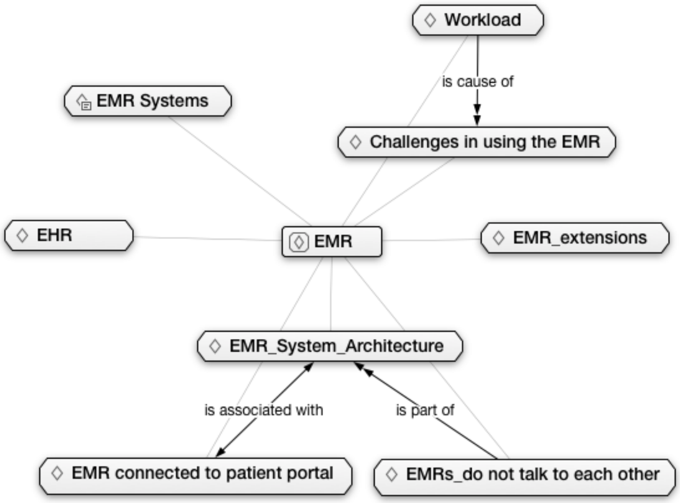


Figure 36. Electronic medical records

We have combined Personal Health Information category and Medical Documents because they share basic information and can be connected to each other through sub-codes as shown in Figure 37.

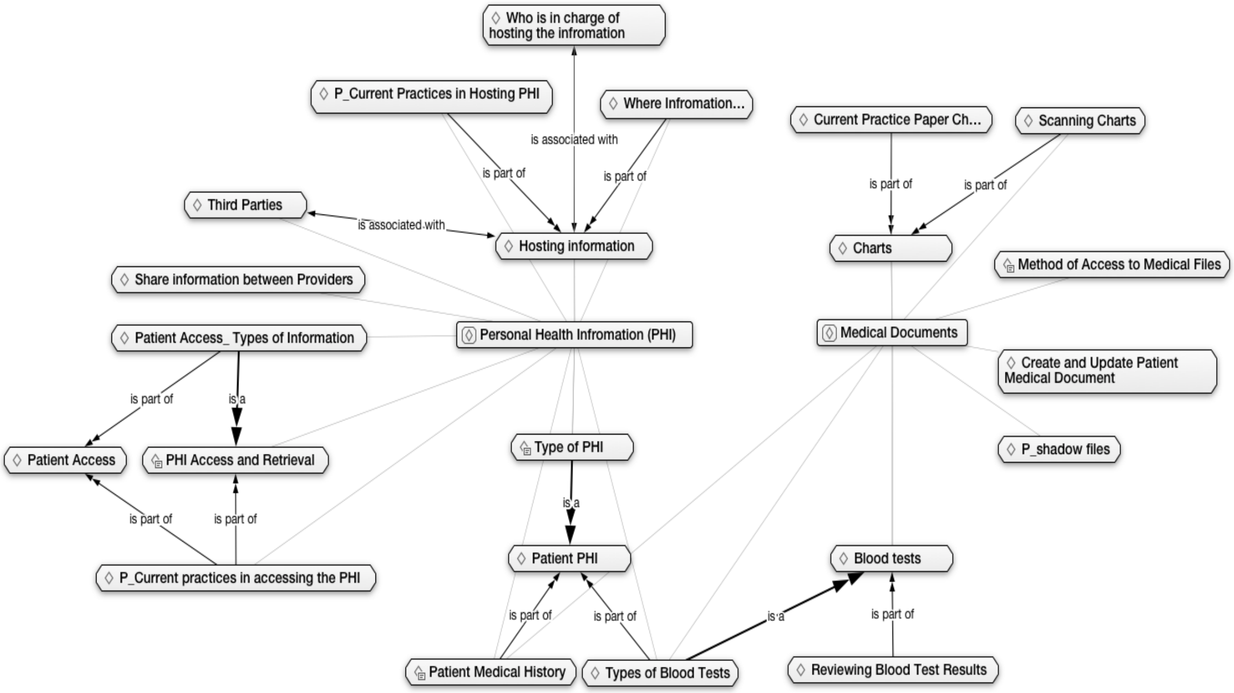


Figure 37. Personal health information and medical documents categories

Another combination between the Online Patients' Portals and Patients Tasks is formed due to the links between sub-codes as shown in Figure 38.

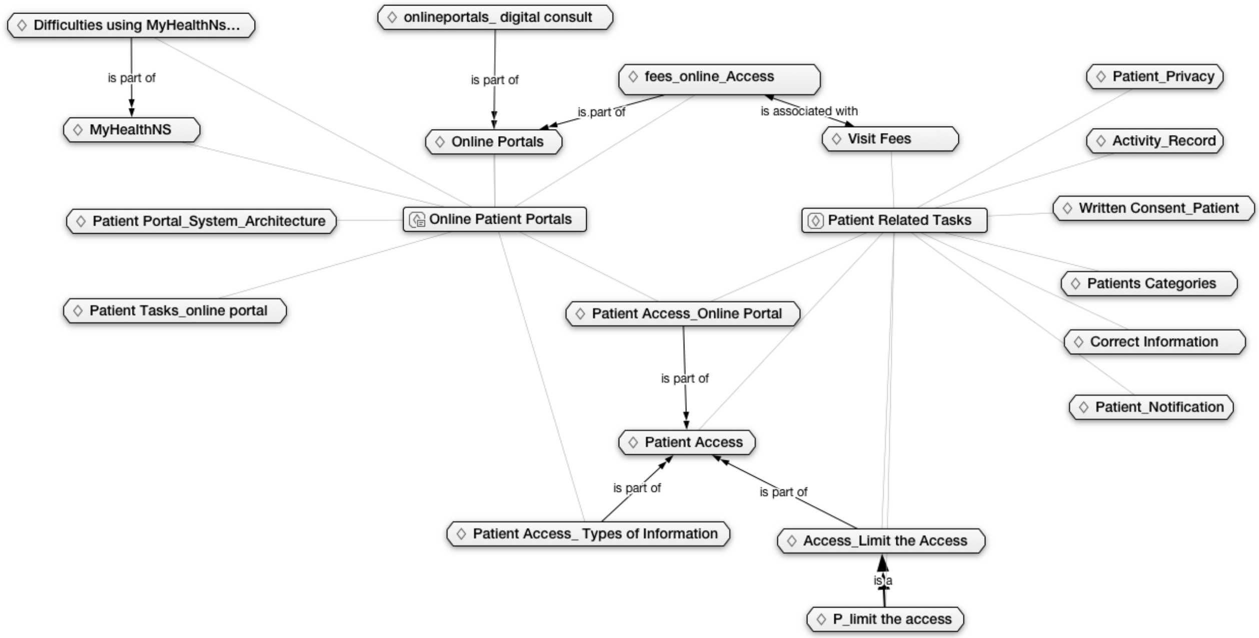


Figure 38. Online portals and patients tasks

Interviewing doctor office admins, I found that they have certain types of tasks and how they perform their tasks is categorized under the Admin practices and tasks code category as shown in Figure 39.

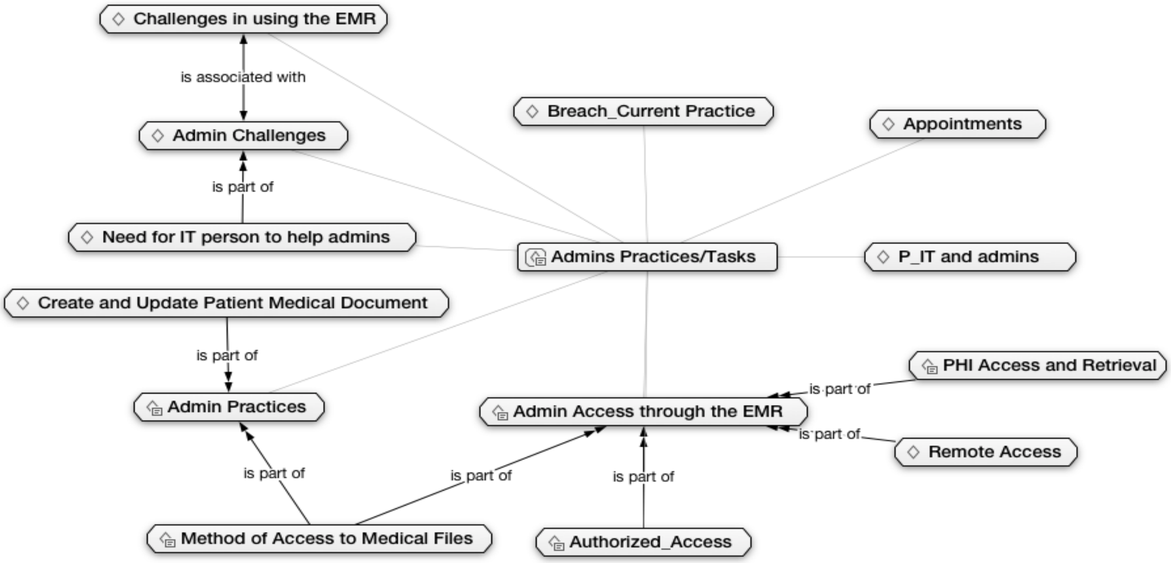


Figure 39. Admins practices and tasks

I have combined the two categories Privacy/NSPHIA compliance with Breach categories as shown in Figure 40.

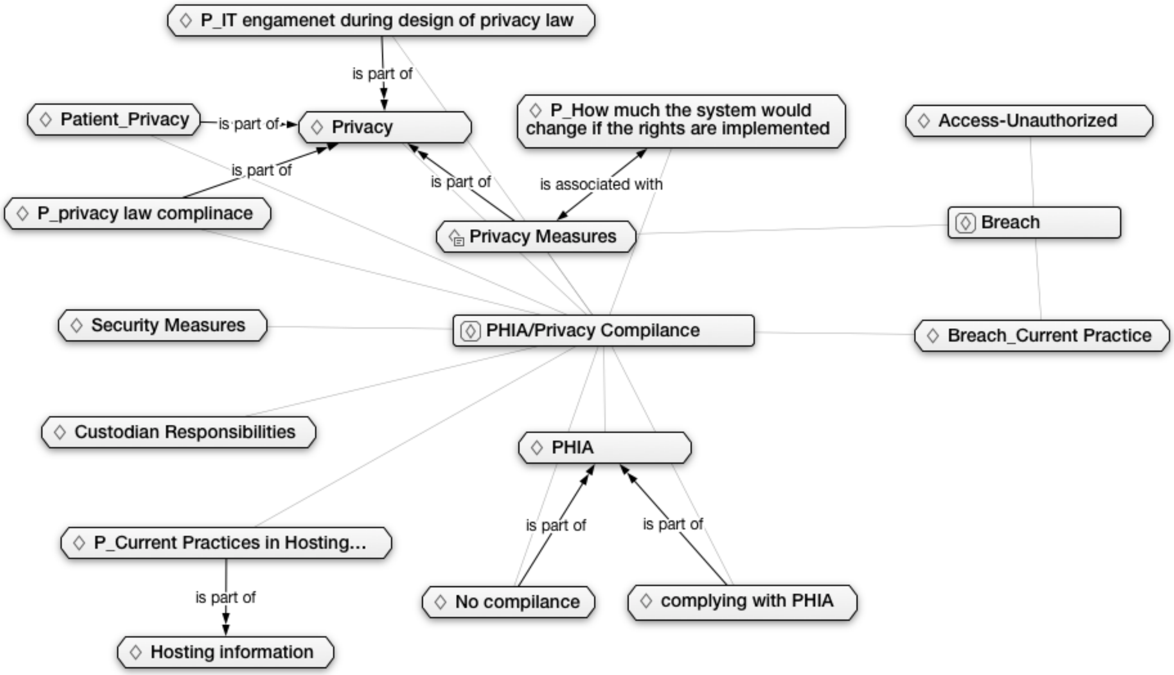


Figure 40. Breach and NSPHIA/privacy compliance categories

Challenges and recommendation categories were combined and include some challenges that admins face regarding the workload and administration practices along with patients' challenges accessing their PHI.

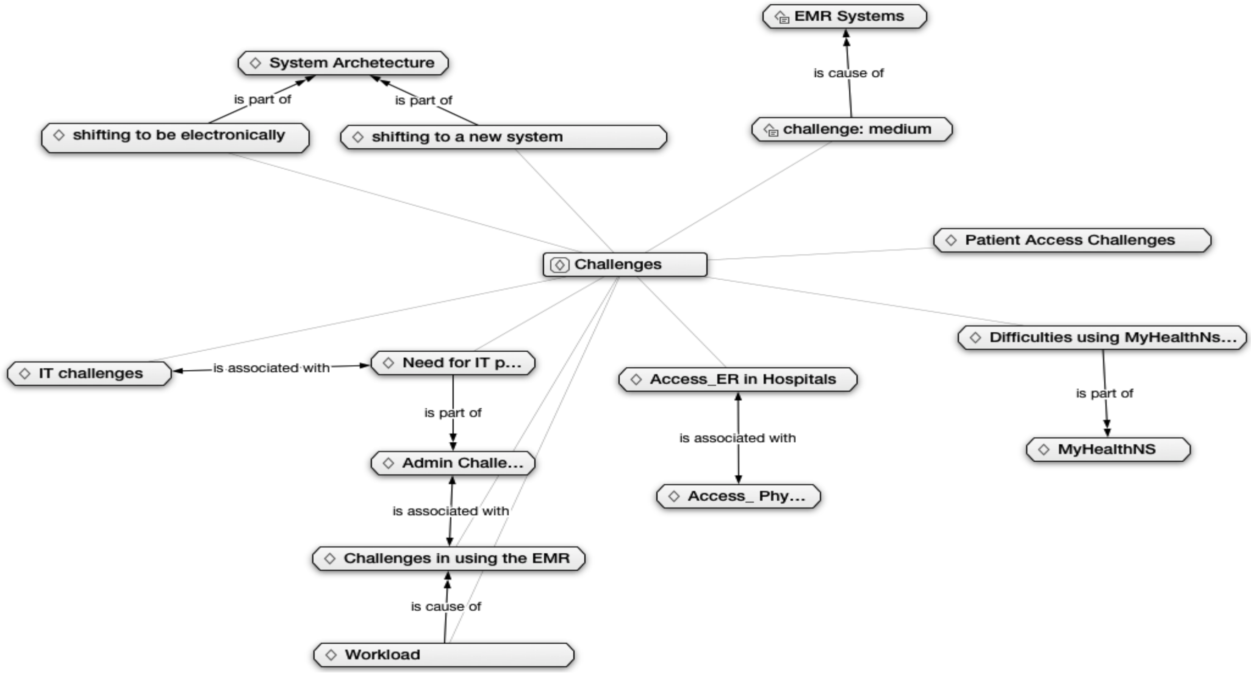


Figure 41. Challenges

Appendix C: The Interview Guide

First Draft:

In-depth Interview Guide
Information Technology (IT) Employees

1. What type of health data are you responsible for processing?

   Probe:

   What do you usually do if you want to (create) and/or (update) an EHR, EMR, or PHI?
2. What types of PHI patients are able to access? Do they have to get access to different types of health information?
3. Who is allowed to access the PHI without patients consent? Why?
4. What type of access is considered as unauthorized? (Allow a discussion with examples or scenarios for the following cases)
   - Access for undefined purposes
   - A physician that I requested not to disclose to
   - Researchers
   - All of them
   - None

   Probe: What consequences should be taken from a technological perspective? any suggestions of from the Legal consequences?
5. What type of PHI that the patient is allowed to correct? Is the corrected information by the patient has to be approved before it is included?
6. If the patient requested not to disclose the information to anyone? What would happen in emergency situations?
7. What is the type of information that patients are allowed to limit the access to? Are they limiting the access to the PHR (aggregated in one place online) or the actual EHR stored internally in the healthcare system?
8. Do third parties manage patients PHI?

   Probes:

   How they process the PHI and EHR? What is the data flow in general?

   If the third party is responsible for storing the health information, hoe patient can get access to their information?

   Are there any security and privacy measures that are applied? What type?
9. What is your biggest struggle in managing the EHRs? What do you think would help overcome the problem?
10. What recommendations do you have for future improvement in managing EHRs?
11. Do you think that the system complies with privacy laws in terms of patients' privacy?

    Probes: What about NSPHIA? If yes, is there a particular process was followed?
12. In case there is am information breach (information was used not for defined purpose, information was stolen or accessed by unauthorized individual)? **Are** patients being informed? **How**?

13. What technology consideration would be taken into account to comply with privacy laws in general and NSPHIA in particular?
14. Data privacy is a growing concern in today's technological landscape, and legislation around safeguarding medical information is particularly strong. How patient privacy is maintained in current practices?

In-depth Interview Guide- Doctors' office administrations

1. What type of health data are you responsible for processing?

   Probe:

   What do you usually do if you want to (create) and/or (update) an EHR, EMR, or PHI?
2. What types of PHI patients are able to access? Do they have to get access to different types of health information?
3. Who is allowed to access the PHI without patients consent? Why?
4. What type of access is considered as unauthorized? (Allow a discussion with examples or scenarios for the following cases)
   - Access for undefined purposes
   - A physician that I requested not to disclose to
   - Researchers
   - All of them
   - None

   Probe-What consequences should be taken from a technological perspective? any suggestions of from the Legal consequences?
5. What is the type of information that patients are allowed to limit the access to? Are they limiting the access to the PHR (aggregated in one place online) or the actual EHR stored internally in the healthcare system?
6. Do third parties manage patients' portals?

   Probes- How they process the PHI and EHR? What is the data flow in general? **If** the third party is responsible for storing the health information, How patient can get access to their information? **Are** there any security and privacy measures that are applied? What type?
7. What is your biggest struggle in managing the EHRs through online/patient portal? What do you think would help overcome the problem?
8. What recommendations do you have for future improvement in managing EHRs through /patient portals?
9. Do you think that the system complies with privacy laws in terms of patients' privacy? What about NSPHIA?

   Probe- If yes, Is there a particular process was followed?
10. What technology consideration would be taken into account to comply with privacy laws in general and NSPHIA in particular?
11. How do you process the patient request to access and correct the PHI? **Probe-** How NSPHIA is complied in processing these two tasks?
12. Are there any network-based healthcare systems or online portals that you think it complies with NSPHIA legislation?

13. In your point of view, Can NSPHIA Legislation be applied in online health-care systems easily? Why or why not? In case there is breach (information was used not for defined purpose, information was stolen or accessed by unauthorized individual)? Are patients being informed? **Probe-** How?
14. How important is engaging IT designers while designing privacy laws?

In-depth Interview Guide- Privacy Professionals

1. What types of PHI patients are able to access? Do they have to get access to different type of health information?
2. Who is allowed to access the PHI without patients consent? Why?
3. Who is allowed to access the PHI without patients consent? Why?
4. What type of access is considered as unauthorized? (Allow a discussion with examples or scenarios for the following cases)
    - o Access for undefined purposes
    - o A physician that I requested not to disclose to
    - o Researchers
    - o All of them
    - o None

    Probe-What consequences should be taken from a technological perspective? any suggestions of from the Legal consequences?
5. What type of PHI that the patient is allowed to correct? Is the corrected information by the patient has to be approved before it is included?
6. What would guarantee that the system provider (custodian) does not allow third parties to access the PHI? What legal consequences should be considered?
7. What conditions are applied to opting in and opting out from consents?

    In the case of stolen information, what are the legal consequences and how they can be applied to/in an online system? The limit of the individual right is to be notified when the situation occurs but it is the organization responsibility to be preventative.

    Probe- What legal consequences should be applied to the organization?
8. Do you think that IT designers would easily understand each right and responsibility and comply it with? Why? Why not?

    Probe- How can we help them?
9. Do you believe that there is a gap between IT designers and privacy law designers?

    Probe-What do you think is cause this gap?
10. How important is engaging IT designers while designing privacy laws?
11. How the healthcare system should insure compliance with privacy laws in general and NSPHIA in particular? **Probe-**Is there any sort of review?
12. What technology consideration would be taken into account to comply with privacy laws in general and NSPHIA in particular? From a legal perspective?
13. What legal consequences are associated in case of not complying?
14. How much would these rights change if we consider EHR and online process through an online portal? What would change and what wouldn't? **Note**: this question was derived

from the recommendation report that Catherine Tully the information & privacy commissioner provided. She said consider EHR practices in the Act. In Sept 2016.

Revised Interview guide:

Interview Guide for Admins:

System Architecture:

1. What type of health data are processed using these EMRs?
2. Are they local office network-based where the EMR is connected to a server and workers and called Local Client Server (LCS).

OR it is an application server provider where the EMR is stored in in data center (online server) and accessed via secure link over the internet?
Or they could be both? Which one are you using?

3. Is your system connected to another system to help you get the information you need (results) ?
4. Is the system that you are using connected to MyHealthNS or the online patient portal?
5. Let's say that there is patient visiting for the first time and you would like to process their health information? What do you do? How is the process?

6. Where the patient data or the PHI is stored using these systems? In Canada?

Access and correction:

7. How do you access the document (name or ID)?

8. What types of PHI patients are able to access? Do they have to get access to different types of health information? lets say that one of the patients came and said I want to access my information?

9. As a patient? I can access everything about me in the online portal? Any type of information?

10. What is the type of information that patients are allowed to limit the access to?
11. Who is allowed to access the PHI without patients consent? Why?
12. What about in emergency situations? ER in hospitals can access information about the patients in your systems?

13. Let's say that a patient while reviewing his/her chart and found that one piece of information is not correct. Can the patient correct the information?

Unauthorized Access and Notification:

14. What type of access to patient information is considered as unauthorized? (Allow a discussion with examples or scenarios for the following cases)
    - Access for undefined purposes
    - A physician that I requested not to disclose to

- Researchers
- All of them
- None

Probe-What consequences should be taken from a technological perspective? any suggestions of from the Legal consequences?

15. Let’s say that patients asked to not disclose their information to anyone (family members, other healthcare providers, if seen by more than one? Is this possible? How it is done through the system is there any kind of features?
16. What other cases you notify patients beside what we have discussed?

Third party hosting the information

17. Do third parties manage patients’ portals?

Probes- How they process the PHI and EHR? What is the data flow in general? If the third party is responsible for storing the health information, How patient can get access to their information? Are there any security and privacy measures that are applied? What type?

18. Do you know where the information is sorted?

Security and Privacy:

19. Are there any security and privacy measures that are applied?
20. Do you believe that privacy is maintained in current practices?

NSPHIA compliance:

21. Have you heard of NSPHIA?
22. Do you think that the system complies with privacy laws in terms of patients’ privacy?

Probe- If yes, Is there a particular process was followed?

23. Let’s say that there is case that there was a breach (information used for undefined purposes, or stolen accessed …..) what would you do as next steps from having this situation
24. Was there any type of updates to ensure compliance?
25. Was it easy? Or difficult?
26. Is there any type of review to make sure that the systems comply with NSPHIA?
27. What technology consideration would be taken into account to comply with NSPHIA ?

Closing remarks:

28. How many patients are connected to MyHealthNS and do they have difficulties?
29. What recommendations do you have for future improvement in managing EHRs?
30. What do you think is preventing doctors from using them?

Interview guide for IT and EMR specialists:

System architecture:

1. What type of health data is processed using these EMRs?
2. Are they local office network-based where the EMR is connected to a server and workers and called Local Client Server (LCS).

OR it is an application server provider where the EMR is stored in in data center (online server) and accessed via secure link over the Internet?
Or they could be both?

3. Can they be connected to MyHealthNS or the online patient portal? Or they can support their own online patient portals as part of the service?
4. Are they connected to the provincial Database? Or the medical records department in hospitals in NS?
5. Can healthcare providers be connected to each other by using these systems or they have to be using the same one to be able to do so?
6. Are they offered just for family healthcare practice or other specialists can have it as well?
7. Where the patient data or the PHI is stored using these systems? In Canada?
8. Do third parties host the information? Is there any kind of review to make sure that they stick with the agreement?

Access:

9. Who is allowed to access the PHI information using these systems?
10. What types of PHI office admins are able to access? Do they have to get access to different types of health information?
11. Are they allowed to access the information without patients consent? Why?
12. Do patients have access? How it the process?
13. Researchers can access the patients PHI?

Unauthorized Access:

14. Do you know if there has been unauthorized access to patients' data using these systems and should happen in this situation?

Patients limiting access:

15. Let's say that patients asked to not disclose their information to anyone (family members, other healthcare providers, if seen by more than one? Is this possible? How it is done through the system is there any kind of features?

Security and Privacy:

16. Are there any security and privacy measures that are applied? What type?
17. How patient privacy is maintained in current practices?

NSPHIA compliance:

18. Have you heard of NSPHIA? When NSPHIA came in some systems where already there and used by physicians?
19. Was there any type of updates to ensure compliance?
20. Was it easy? Or difficult?
21. Is there any type of review to make sure that the systems comply with NSPHIA?
22. What technology consideration would be taken into account to comply with NSPHIA?

General closing remarks:

23. What recommendations do you have for future improvement in managing EHRs?

Appendix D: The Cooperative Prototyping List of Tasks

The tasks are organized under main categories including: Data Collection, Notice/Notification, Consent, Access and Information Disclosure.

Notes:

- An activity record is a list of all stakeholders and healthcare providers, who have accessed, viewed, added, modified, sent and printed PHI of a patient using the online portal.
- Privacy principles are the classification of ISO 29100 privacy Framework.
- Each privacy pattern covers a privacy right from NSPHIA.

Category 1: Notice/Notification and Data Collection Tasks

What should a notification include?
How to communicate details in a UI element?
What type of notification is a high, medium, or low risk?
What type of design considerations to represent solutions?

No.	Privacy principle	Task	Scenario	Privacy pattern	Notes during prototype	Next/following Task
1	Collection Limitation	Collecting PHI	When the patients' PHI is collected for defined purposes	P1 P4	•Who accessed •When •Patient consent	Reviewing the activity record
2	Collection Use, Retention and Disclosure limitation	Secondary use of information	The patient s PHI was collected for undefined purposes	P1 P3 P4	•Who accessed •When •Why •Patient consent	•Reviewing the activity record •Limiting Disclosure task
3	Accountability Breach	Unauthorized access	The patient either found that his/her information was subjected to unauthorized access or/and	P1 P4	•Who accessed •When •Why	•Next steps taken to recover from the breach
4	Accountability Breach	Unauthorized modification	The patient wants to be notified/informed when there is a detected unauthorized access	P1 P2 P3	•Who, When, What type of information is subjected. •Third parties •Healthcare professional	•Reviewing the activity record AND •Correction task •Review agreement

No.	Privacy principle	Task	Scenario	Privacy pattern	Notes during prototype	Next/following Task
5	Accountability Use, Retention and Disclosure limitation	PHI was disclosed	The patient want to be informed when their PHI is disclosed to be able to review the list and apply restrictions	P4 P3	•Disclosure outside NS •Inside NS	•Consent/review agreement •Review activity record •Limit Disclosure

Table 19. Notice/Notification and Data Collection Tasks

Category 2: Data Access
What forms of data representation should be applied?
How important is performing these tasks?
What they are able to access and what they are not?
Is the representation interactive? Or informative?

No.	Privacy principle	Task	Scenario	Privacy pattern	Condition/Note	Next/following Task
6	Individual Participation and Access Openness, transparency and notice	Access PHI	The patient wants to access their personal health information a and review what is collected about them	P1 P2	•How •Authentication techniques that best fit patient's needs •What sources of information EHR, EMR, tests, imaging, etc.	•Review agreement •Review activity record
7	Accuracy and quality Openness, transparency and notice	Correct PHI	The patient found that part of their PHI is not correct and they want to correct it.	P1 P2	•How •What type of information needs to be reviewed by healthcare providers and what does not need to be reviewed?	•Wait for review •Upload documents •Notification of changes in the PHR
8	Accuracy and quality Openness, transparency and notice	Check PHI is up-to-date	The patient found that their information is not up-to-date and they want to add dome information	P1 P2	•How •What type of PHI that they are allowed to add by themselves •Waiting for the review	Add PHI task

No.	Privacy principle	Task	Scenario	Privacy pattern	Condition/Note	Next/following Task
9	Accuracy and quality Openness, transparency and notice	Add PHI to the record	The patients want to add more information to their records	P1	•How they are marked that it is from patients not healthcare providers	Non

Table 20. Data Access Tasks

Category3: Information Disclosure
When information is disclosed?
To whom information are disclosed with and without consent?
How can end-users practice their privacy rights in dealing with the list in the activity record?

No.	Privacy principle	Task	Scenario	Privacy pattern	Condition/Note	Next/following Task
10	Consent and Choice Purpose Legitimacy and Specification Activity record	Setting a pre-defined list of providers and custodians	The patient is interested in specifying a pre-defined list in which a certain number of healthcare providers and agents can access their information or collect them.	P3 P2	•How •What consequences they need to know before applying this feature •When they can and when they cannot	•Activity record •Notification
11	Consent and Choice Purpose Legitimacy and Specification Activity record	Limit the list in the activity record	The patient found after reviewing the activity record is that they want to either hide part of the information or want to apply restrictions and limit the list of agents	P3 P4	•How •What consequences they need to know before applying this feature •When they can and when they cannot	Notification
12	Consent and Choice Purpose Legitimacy and Specification	Request to block all	The patient wants to apply a feature of blocking all information.	P3 P2	•A discussion of consequences •When and what type of PHI they can apply the block all.	•Notification •Consent to responsibilities for block all

Table 21. Information Disclosure Tasks

Category 4: Consent
What should a consent UI representation include?
How these information is communicated?
Is the consent well-informed and clear?
What type of UI representation is ideal in our context?
Type of the follow up notification: high, medium, low risk?

No.	Privacy principle	Task	Scenario	Privacy pattern	Condition/Note	Next/following Task
13	Consent and Choice	Agreement on custodian privacy policy	A patient wants to review the custodian's privacy policy.	P1 P2 P3 P4	•What information •Opting in and out •Time stamp •Negotiation	Notification of changes
14	Consent and Choice Purpose Legitimacy and Specification	Agreement to collect Information	Patients want to know who is doing the collecting of their PHR and for what purpose to be able to decide whether to give consent or not.	P1 P2 P3 P4	•What information •Opting in and out •Time stamp •Negotiation	•Notification of changes •List of custodians who can and cannot access after the update
15	Consent and Choice	Agreement to third party	The patient wants to opt in and opt out from an agreement with the third party in case their information is outsourced.	P1 P2 P3 P4	•What information •Opting in and out •Time stamp •Negotiation	•Informative notification

Table 22. Consent Tasks

Appendix E: Pre- and Post-Study Questionnaire

Pre-Study Questionnaire
Participant ID: ………..

1. **Age (in years) ………………….**
2. **Sex:**
   - ○ Male
   - ○ Female
   - ○ Other / Prefer not to answer

3. **What is the highest level of education that you have completed or are in the process of completion?**

   - ○ High School
   - ○ Bachelor's Degree
   - ○ Master's Degree
   - ○ Doctoral Degree (e.g. PhD, D.Phil)
   - ○ Professional Degree (e.g. MD, LLB, JD, B.Eng)
   - ○ Other

   If other, please specify……………………………………………….

4. **If working (part-time or full-time), what is your occupation?**
   ……………………………………………………………………………………………….

5. **If you are working as a privacy professional, doctor office administrator, human factors professional or an IT designer, how many years of experience do you have?**
   - ○ None
   - ○ One year
   - ○ At least 1 but less than 3 years
   - ○ At least 3 but less than 5 years
   - ○ At least 5 but less than 10 years
   - ○ More than 10 years

Post- Study Questionnaire

7. What could be integrated as design requirement and what could not? Why?
8. What challenges might designers face in integrating these requirements? Why? What suggestions do you have to overcome these challenges? From IT perspective or privacy perspective?
9. What challenges might be associated with these requirements? Are they feasible (do-able)?
10. What benefits do you think these requirements will bring to the design of Online Patient Portals or online Personal Health Records?
11. Do you have challenges in communicating your experiences and background during the prototyping with other participants from different areas and background?
12. How do you describe your experience?

Appendix F: Glossary

Agent

Agent, in relation to a custodian, means a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian, and includes, but is not limited to, an employee of a custodian or a volunteer who deals with personal health information, a custodian's insurer, a lawyer retained by the custodian's insurer or a liability protection provider.

Collect

Collect, in relation to personal health information, means to gather, acquire, receive, gain access to or obtain the information by any means from any source. consent. Agreement by the individual for the entity to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. Explicit consent is given orally, electronically, or in writing, is unequivocal and does not require any inference on the part of the entity seeking consent. Implicit consent may reasonably be inferred from the action or inaction of the individual such as not having opted out, or providing credit card information to complete a transaction.

Custodian

Custodian means an individual or organization described below who has custody or control of personal health information as a result of or in connection with performing the person's or organization's duties.

Disclose

Disclose, in relation to personal health information in the custody or under the control of a custodian or a person, means to make the information available or to release it to another custodian or to another person, but does not include to use the information.

Data Subject (DS)

An individual or a person who has the rights to share, manage and control personal information.

Data Controller (DC)

The person who decides in which and how data are processed.

Data Processor (DP)

A person or an individual who process data on behalf of the data controller.

Third party (TP)

Agent that is not affiliated with the custodian that collects personal information or any affiliated agent not covered by the agent's privacy notice. Any person or organization other than data subject, processor, and controller.

Health care

Health care means an observation, examination, assessment, care, service or procedure in relation to an individual that is carried out, provided or undertaken for one or more of the following health related purposes: the diagnosis, treatment or maintenance of an individual's physical or mental condition, the prevention of disease or injury, the promotion and protection of health, palliative care, the compounding, dispensing or selling of a drug, health-care aid, device, product, equipment or other item to an individual or for the use of an individual, under a prescription, or a program or service designated as a health-care service in the legislation.

Identifying information

Identifying information means information that identifies an individual or, where it is reasonably foreseeable in the circumstances, could be utilized, either alone or with other information, to identify an individual.

Individual

Individual, in relation to personal health information, means the individual, whether living or deceased, with respect to whom the information was or is being collected or created. The person about whom the personal information is being collected (sometimes referred to as the data subject).

Personal health information

Personal health information means identifying information about an individual, whether living or deceased, and in both recorded and unrecorded forms, if the information relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, relates to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual, relates to payments or eligibility for health care in respect of the individual, relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, is the individual's registration information, including the individual's health-card number, or identifies an individual's substitute decision-maker.

Privacy breach

A privacy breach occurs when personal information is collected, retained, accessed, used, or disclosed in ways that are not in accordance with the provisions of the enterprise’s policies, applicable privacy laws, or legislation.

Purpose

The reason personal information is collected.

Record

Record means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Review Officer

Review Officer means the Privacy Review Officer under the Privacy Review Officer Act.

Receiver

A person to whom data are disclosed and can be a third party or any other individual.

Use

Use, in relation to personal health information in the custody or under the control of a custodian or a person, means to handle or deal with the information, but does not include disclosing the information.

Opt in

Personal information may not be collected, used, retained and disclosed by the entity without the explicit consent of the individual.

Opt out

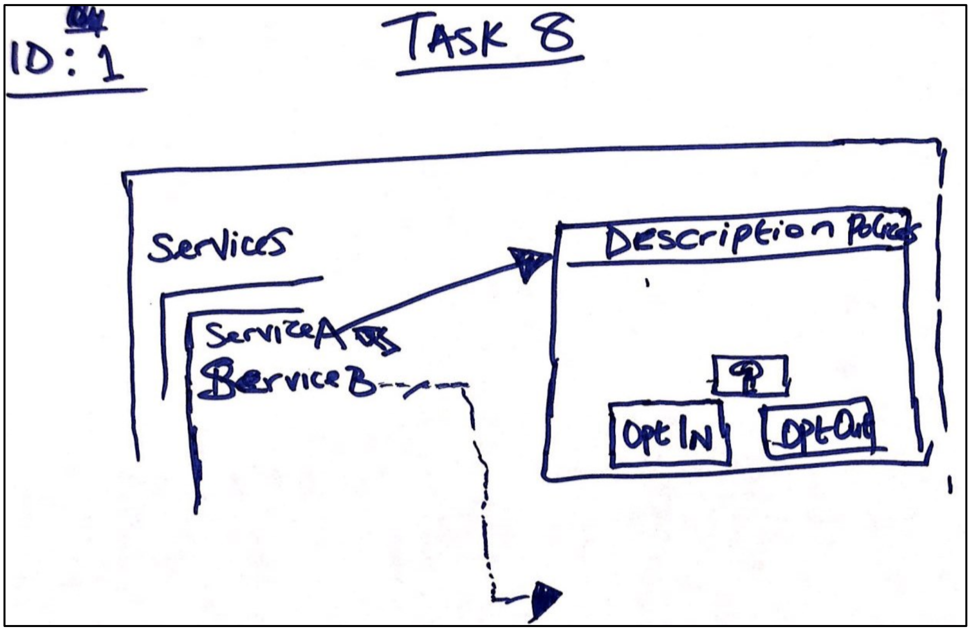
Implied consent exists for the custodian or agent to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

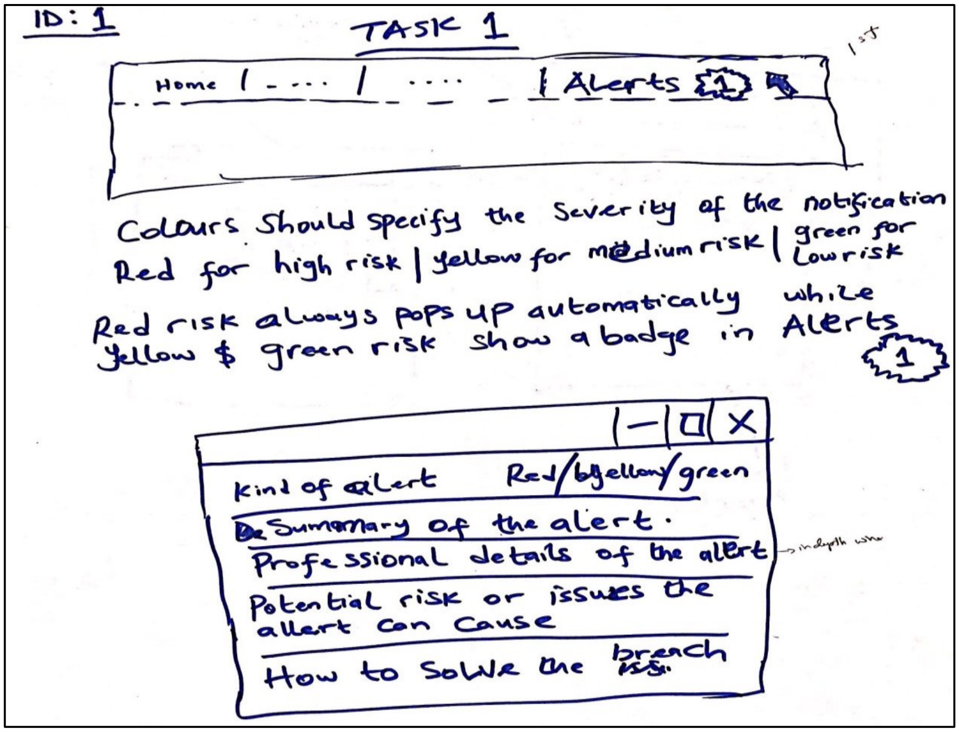
Outsourcing

The use and handling of personal information by a third party that performs a business function for the entity.

Appendix G: Participants’ Sketches

Initial CARD sessions





Colours Should specify the Severity of the notification

Red for high risk | yellow for medium risk | green for Low risk

Red risk always pops up automatically while yellow $ green risk show a badge in Alerts

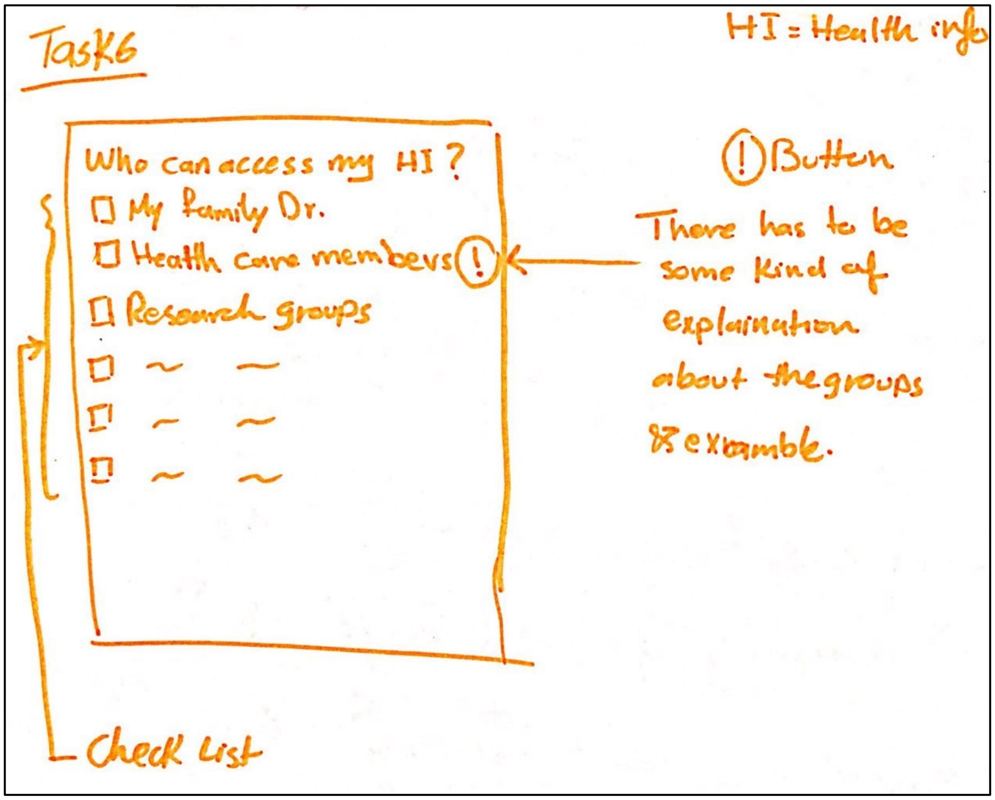
Kind of alert Red/yellow/green

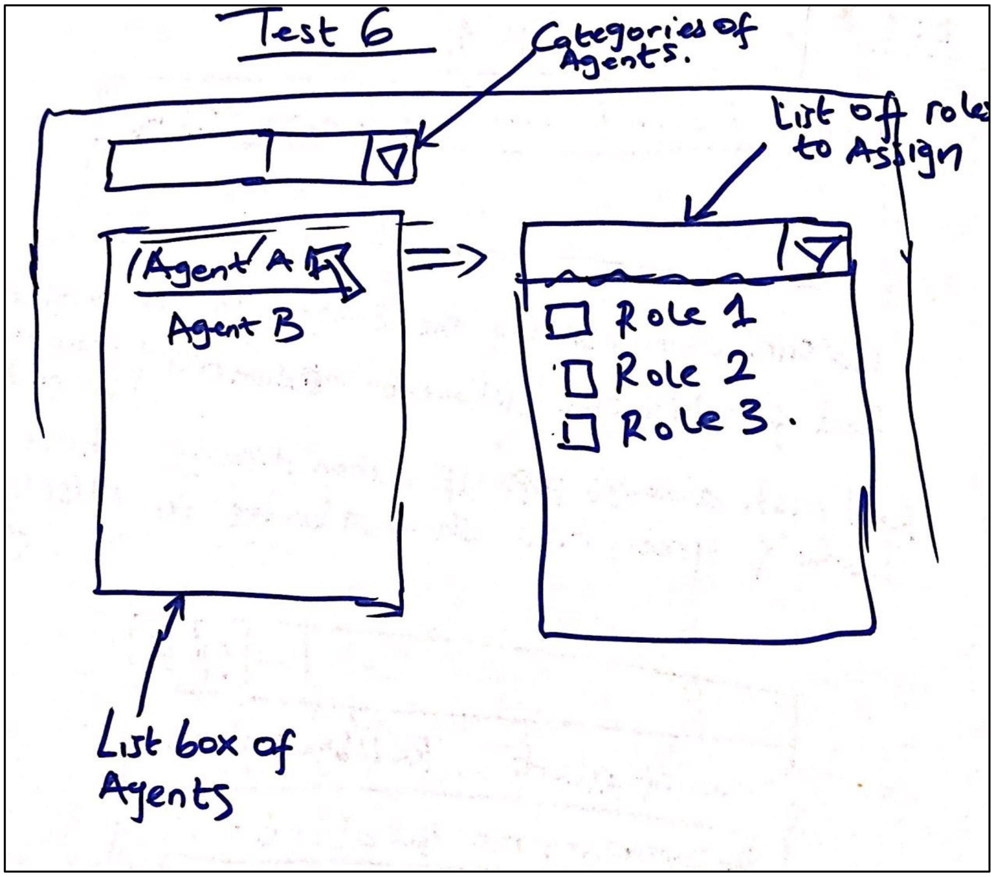
Summary of the alert.

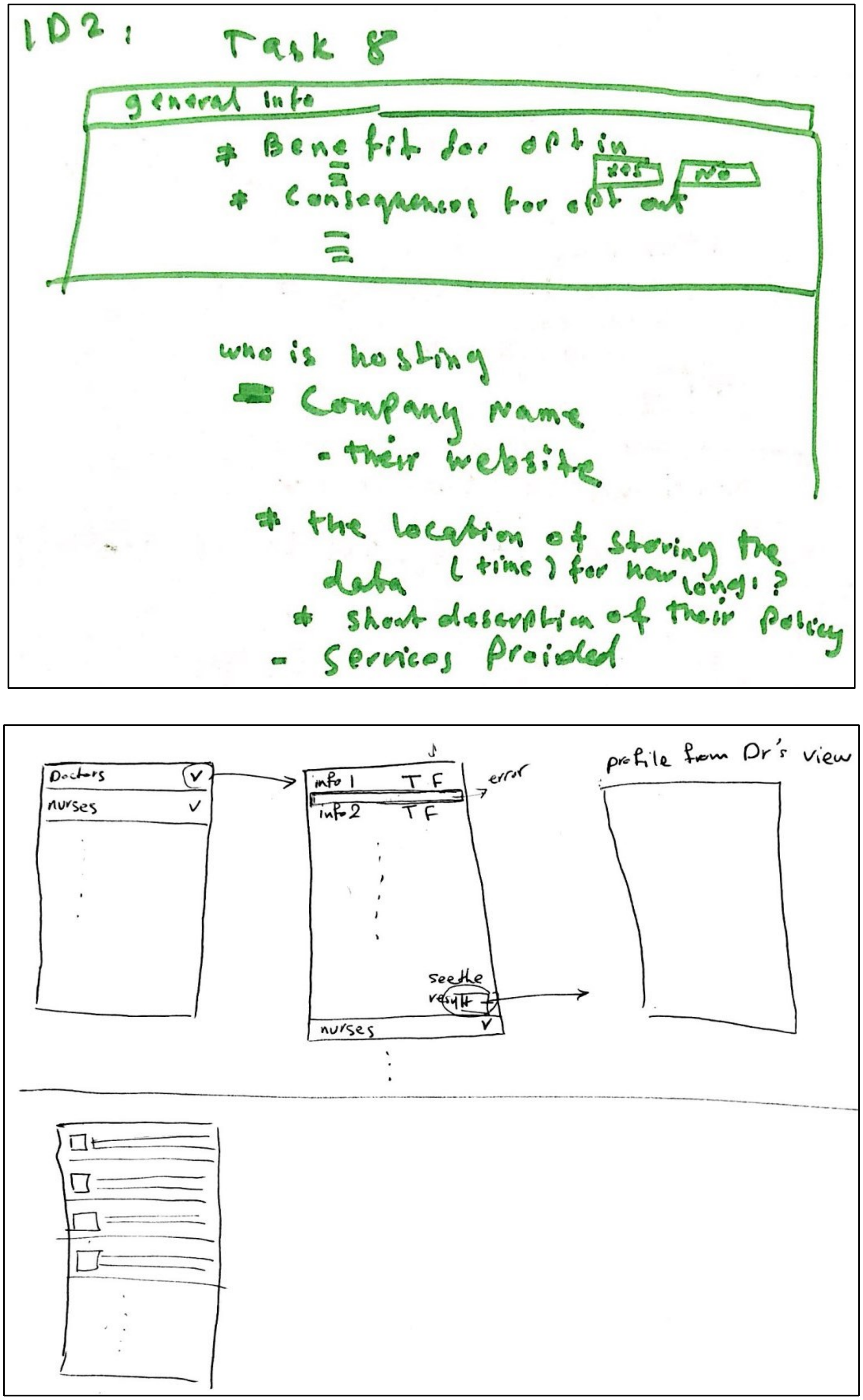
Professional details of the alert → in depth what

Potential risk or issues the allert can cause

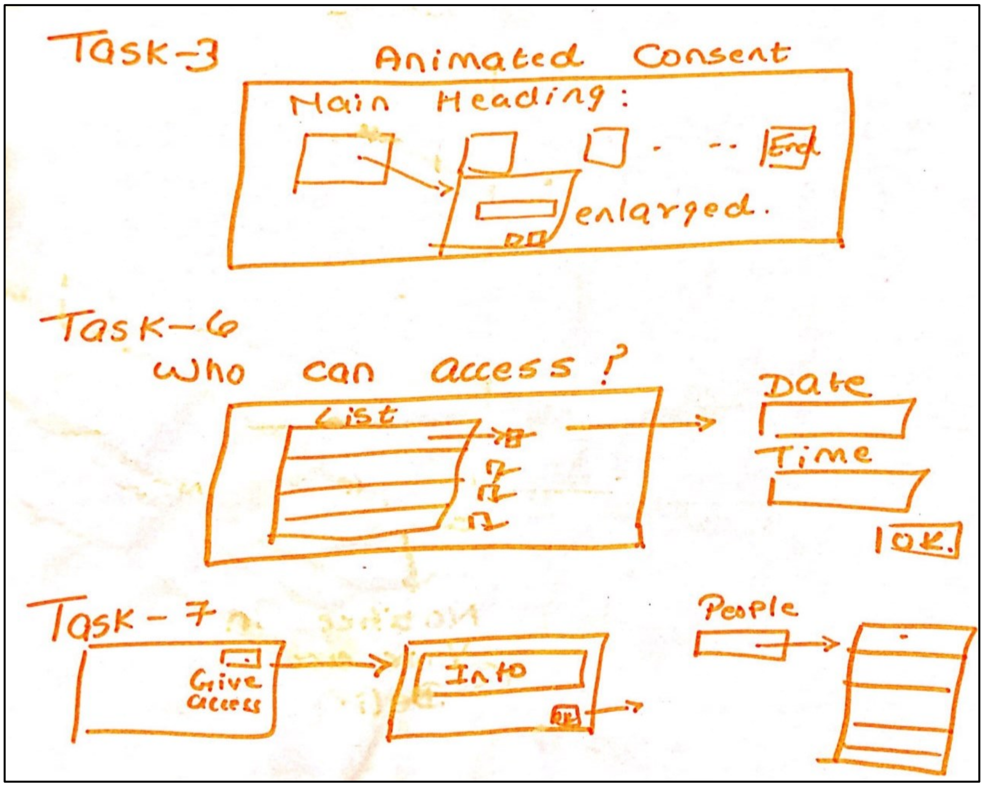
How to Solve the breach


Task6
HI = Health info
Who can access my HI?
□ My family Dr.
□ Heatth care members (!)
□ Research groups
□ ~ ~
□ ~ ~
□ ~ ~
(!) Button
There has to be some kind of explaination about the groups & examble.
Check List

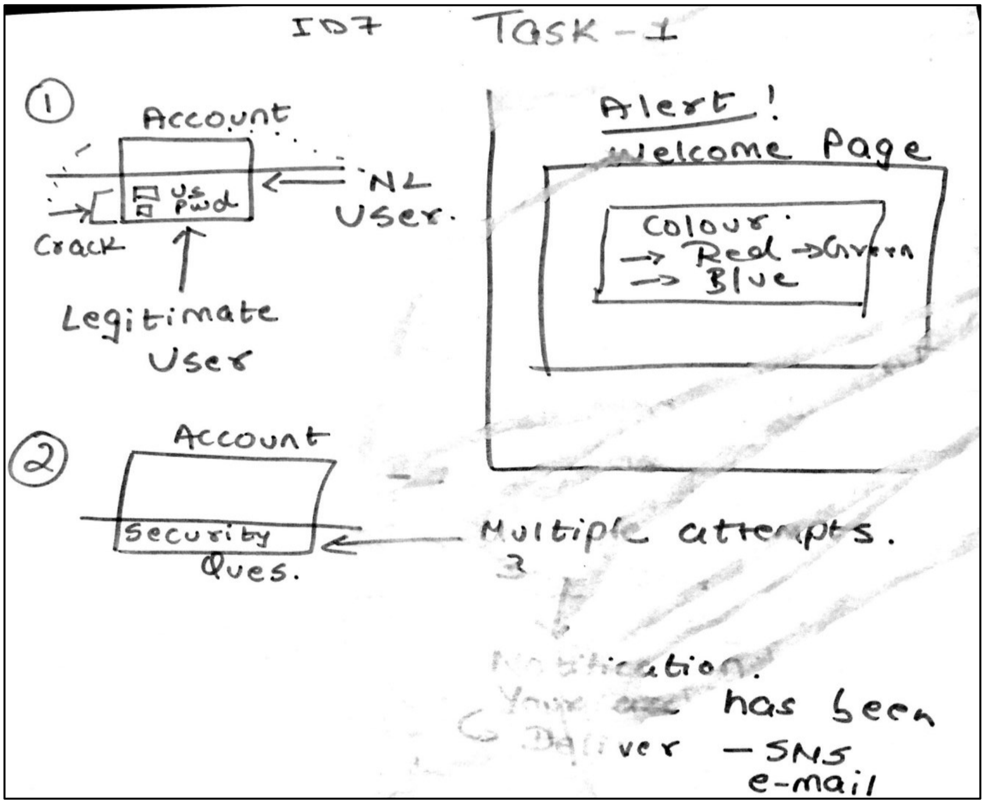

Test 6
Categories of Agents.
List of roles to Assign
Agent A
Agent B
□ Role 1
□ Role 2
□ Role 3.
List box of Agents

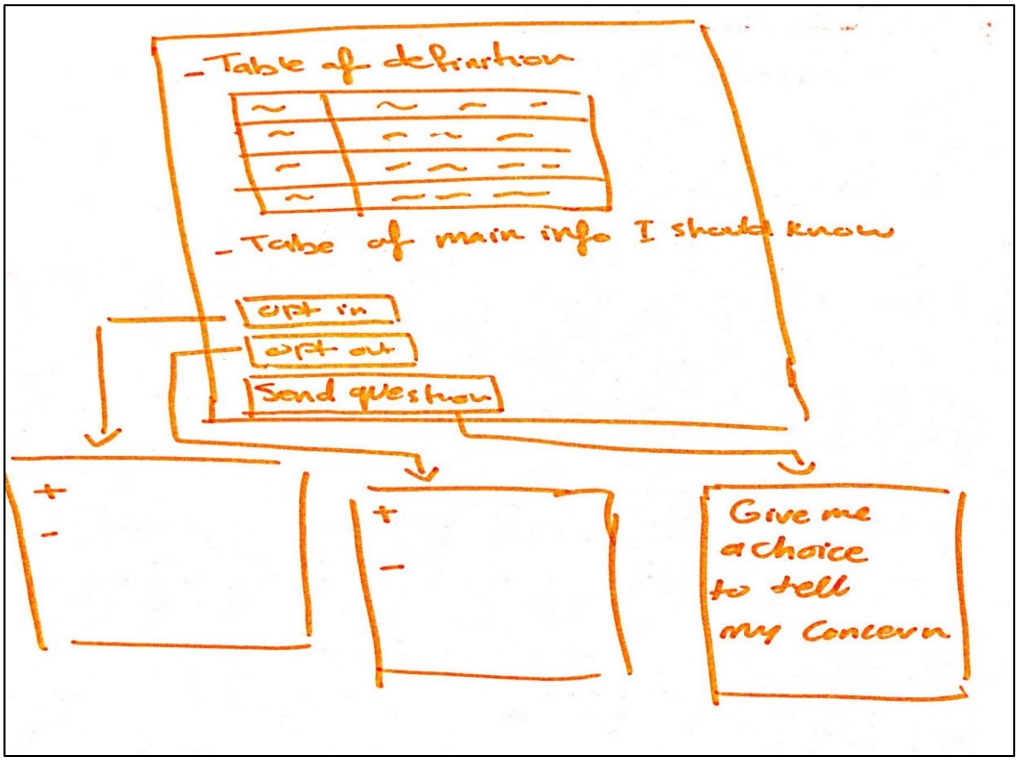


ID Participant 9 Sketch.

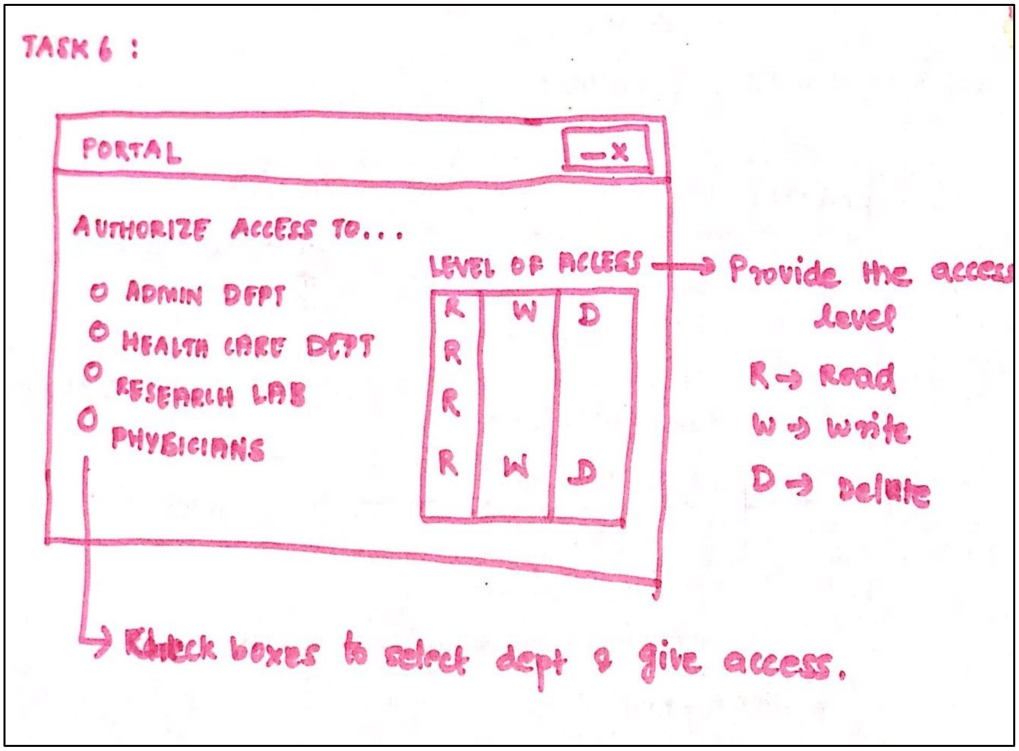


ID Participant 11 Sketch.

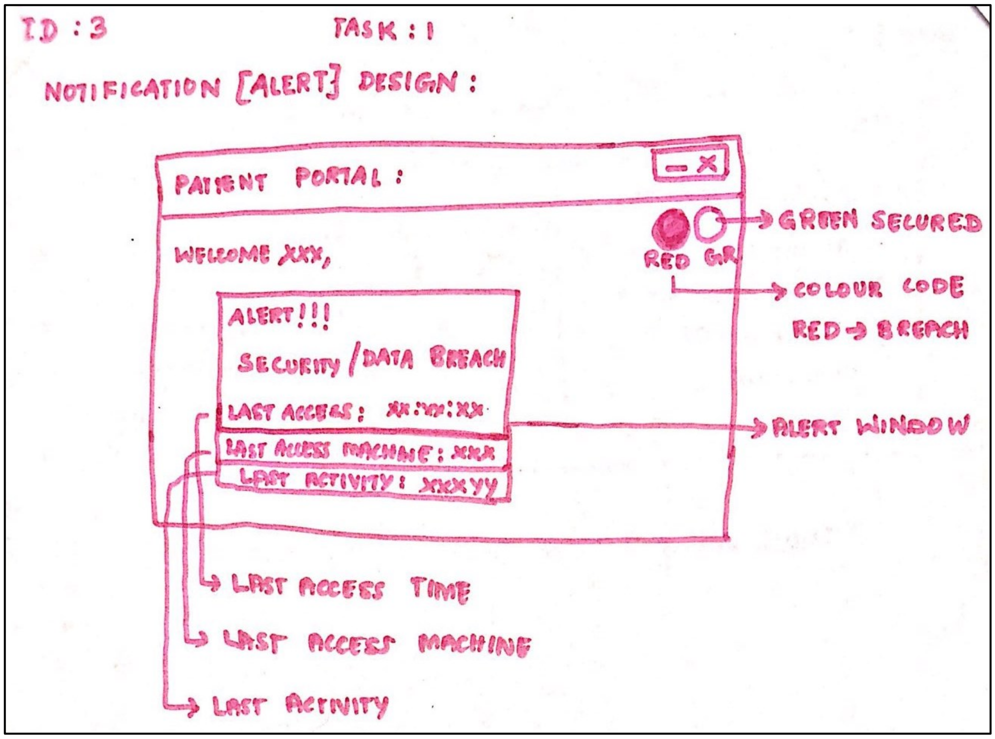



- Table of definition
- Table of main info I should know
opt in
opt out
Send question
+
-
+
-
Give me a choice to tell my concern

ID Participant 4 Sketch.



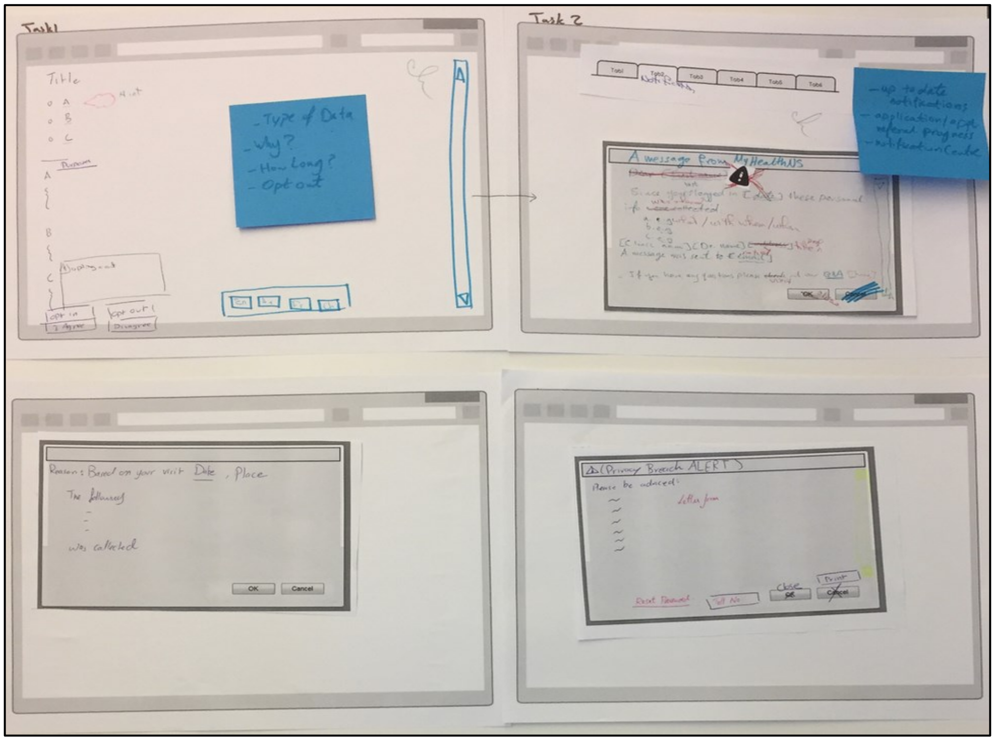
ID Participant 3 Sketch



ID Participant 3 Sketch

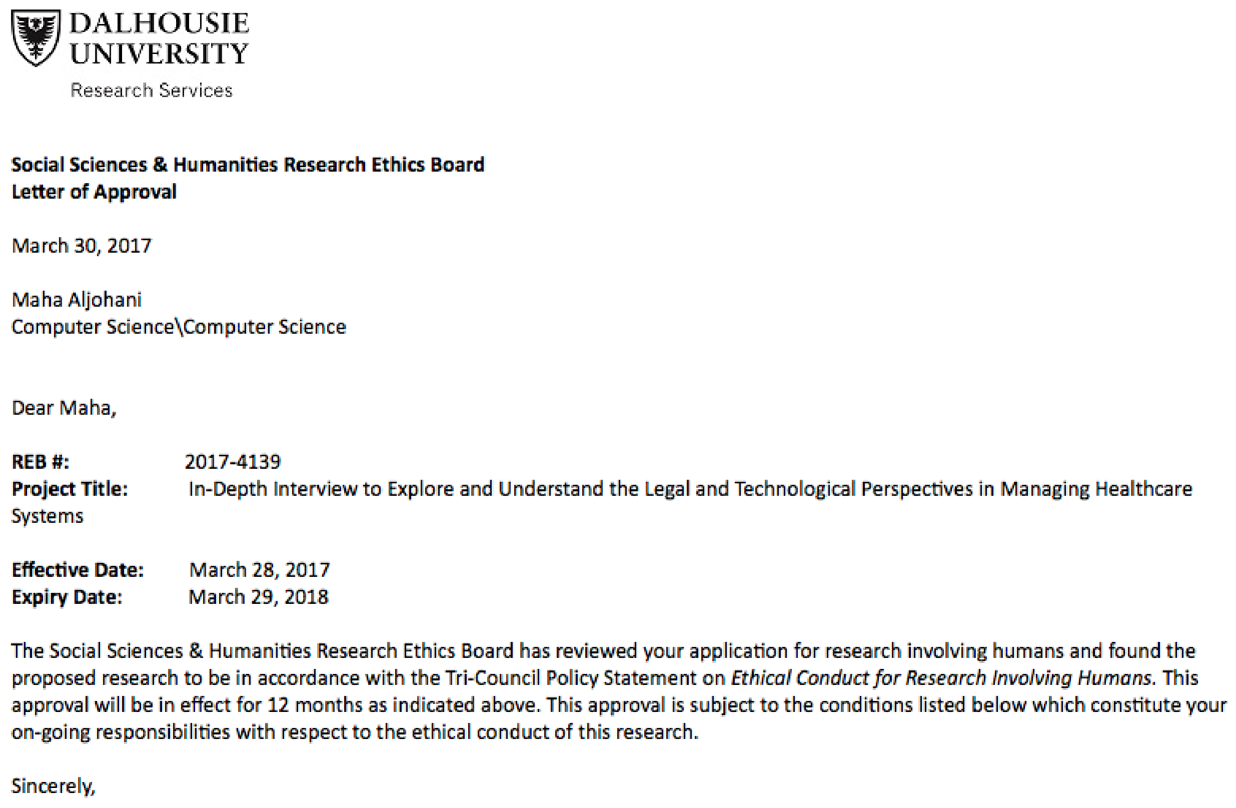
Decision Making Workshops Sketches

- DM workshop Round one with a privacy professional



Appendix H: Dalhousie REB approval letters

1- Interview Study



DALHOUSIE
UNIVERSITY
Research Services

Social Sciences & Humanities Research Ethics Board
Letter of Approval

March 30, 2017

Maha Aljohani
Computer Science\Computer Science

Dear Maha,

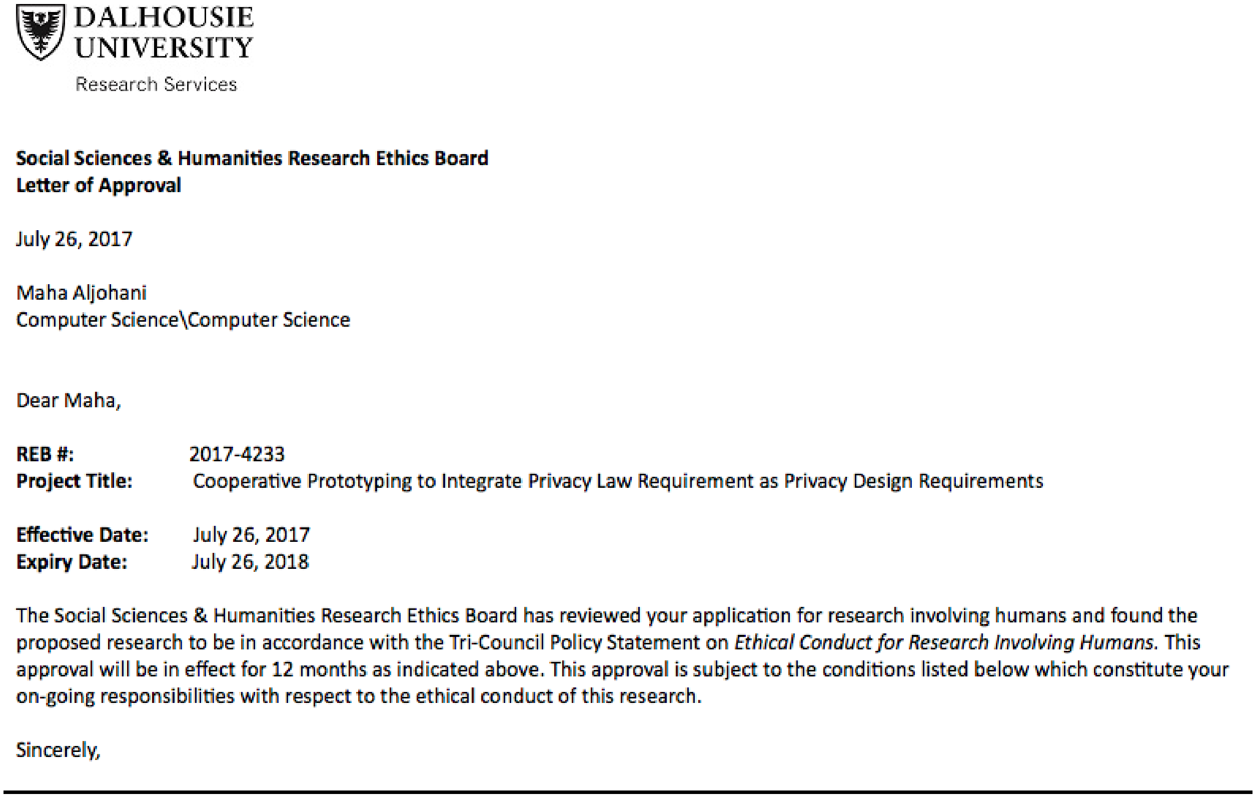
REB #: 2017-4139
Project Title: In-Depth Interview to Explore and Understand the Legal and Technological Perspectives in Managing Healthcare Systems

Effective Date: March 28, 2017
Expiry Date: March 29, 2018

The Social Sciences & Humanities Research Ethics Board has reviewed your application for research involving humans and found the proposed research to be in accordance with the Tri-Council Policy Statement on *Ethical Conduct for Research Involving Humans.* This approval will be in effect for 12 months as indicated above. This approval is subject to the conditions listed below which constitute your on-going responsibilities with respect to the ethical conduct of this research.

Sincerely,

2- Cooperative Prototyping Study



DALHOUSIE
UNIVERSITY
Research Services

Social Sciences & Humanities Research Ethics Board
Letter of Approval

July 26, 2017

Maha Aljohani
Computer Science\Computer Science

Dear Maha,

REB #: 2017-4233
Project Title: Cooperative Prototyping to Integrate Privacy Law Requirement as Privacy Design Requirements

Effective Date: July 26, 2017
Expiry Date: July 26, 2018

The Social Sciences & Humanities Research Ethics Board has reviewed your application for research involving humans and found the proposed research to be in accordance with the Tri-Council Policy Statement on *Ethical Conduct for Research Involving Humans.* This approval will be in effect for 12 months as indicated above. This approval is subject to the conditions listed below which constitute your on-going responsibilities with respect to the ethical conduct of this research.

Sincerely,