Treading the Line:
Seeking balance in information sharing and privacy in *ActionADE*

by

Serena Small

B.A. (Hons), Carleton University, 2013

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Communication
Faculty of Communication, Art, and Technology

SIMON FRASER UNIVERSITY
Summer 2017

Approval

Name:	**Serena Small**
Degree:	**Master of Arts**
Title:	**Treading the Line: Seeking balance in information sharing and privacy in *ActionADE***
Examining Committee:	**Chair: J. Adam Holbrook** Adjunct Professor
	Ellen Balka Senior Supervisor University Professor
	Peter Chow-White Supervisor Associate Professor
	John Calvert External Examiner Associate Professor Faculty of Health Sciences
Date Defended/Approved:	July 13, 2017

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Patient data in health care offers both opportunities and challenges that benefit from study through a sociotechnical lens. This thesis examines issues related to data sharing and privacy in the context of the development and implementation of *ActionADE*, a system designed to enable the communication and documentation of adverse drug events (ADEs), which are the harmful and unintended consequences of medication use. This thesis first explores the current policy environment surrounding health data privacy in British Columbia as it relates to *ActionADE*, and then contributes patient perceptions and attitudes about data sharing and privacy in the context of *ActionADE* through an analysis of focus group data. This thesis results in a series of recommendations for *ActionADE*, in order to identify information sharing preferences, privacy concerns, and policy constraints at the outset, striking a balance between the need to both disclose and protect personal health information.

Keywords: health data; information and communication technologies; data privacy; public policy; adverse drug events; patient perceptions

Acknowledgements

Thank you to Ellen Balka for her ongoing support, guidance, and encouragement. The opportunity to work for and with Ellen has helped me grow personally and professionally. I am deeply grateful for her perpetual enthusiasm and willingness to support my endeavours and interests.

Thank you to the rest of the *ActionADE* team: Corinne Hohl, David Peddie, Christine Ackerley, Amber Cragg, Maeve Wickham, Stephanie Woo, Jeffrey Hau, Chantelle Bailey, and Katherin Badke. I have learned so much from each of them. I am especially thankful for the support of David Peddie, for guiding me through the thick of graduate school.

Thank you to the friends that have become family in a new city: Annelisa Lott, Hayley Dobson, Jacob Chila, and many more.

Above all, thank you to my family, Kevin Small, Fiona Keith, and Norma Stansbury. Thank you for endless love, support, and patience from across the country.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ADEs	Adverse drug events
ADRs	Adverse drug reactions
BC	British Columbia
BCCLA	British Columbia Civil Liberties Association
CHT	Canada Health Transfer
CI	Contextual Integrity
CIHI	Canadian Institutes of Health Information
CPIC	Canadian Police Information Centre
ED	Emergency department
EHRs	Electronic health records
EMRs	Electronic medical records
FBI	Federal Bureau of Investigation
FIPA	Freedom of Information and Privacy Association
FIPPA	Freedom of Information and Protection of Privacy Act
GP	General practitioner
HIPPA	Health Insurance Portability and Protection Act
ICD-10	International Statistical Classification of Diseases and Related Health Problems (10th Revision)
ICTs	Information and communication technologies
MSP	Medical Services Plan
NSA	National Security Agency
OIPCBC	Office of the Information and Privacy Commissioner for British Columbia
PHAC	Public Health Agency of Canada
PIPA	Personal Information Protection Act
PIPEDA	Personal Information Protection and Electronic Documents Act
RCMP	Royal Canadian Mounted Police
SARS	Severe acute respiratory syndrome
SCOT	Social construction of technologies
STS	Science and technology studies
US	United States
VCH	Vancouver Coastal Health
VGH	Vancouver General Hospital

Chapter 1.

Introduction & Thesis Overview

In health, the availability and accessibility of patient information is essential to the delivery of care. Affording clinicians the knowledge of patient medical histories, preferences, social circumstances, and so forth, may play a critical role in both short and long term patient care and health outcomes. It is through this perspective that the rise of electronic medical records (EMRs) and other information and communication technologies (ICTs) in health have been perceived and presented as the saving grace for a health system that is otherwise characterized by fragmentation, both in terms of the provision of care (e.g., hospital care providers versus community-based physicians and specialists working in different jurisdictions) and in the systems that enable care (e.g., hospital and community EMRs that are not interoperable).

Consider, for example, the case of a diabetic patient who presented comatose at Hospital A due to critically low blood glucose levels resulting from their prescription for glyburide (Balka, 2014). At the point of discharge from the hospital, the patient was instructed to stop glyburide and was prescribed a similar medication, gliclazide, which has a lower risk of negatively affecting blood glucose levels (Balka, 2014). Shortly thereafter, the patient presented at Hospital B with the same diagnosis (Balka, 2014). A clinical pharmacist completed a medication review with the patient and found that the patient had been dispensed both gliclazide and glyburide (Balka, 2014). It became evident that the patient had not understood the discharge instructions from Hospital A, and the patient's community pharmacist and family physician had not been alerted to the new prescription and discontinuation instruction, as no system - electronic or otherwise - was in place to bridge gaps in informational continuity associated with geography and jurisdiction (Balka, 2014). In this example, the lack of communication between the hospital and community pharmacy was life threatening. Hindsight offers the view that effective communication processes and systems could have prevented such an event.

Although improved information sharing might reduce the occurrence of such incidences, the desire for increased sharing and availability of health information has significant implications. In the context of ICTs beyond the health domain, increased

access and sharing of personal information is coupled with concern regarding the implications on individual privacy. Furthermore, in the health domain in particular, the information that is being collected, used, and shared is often viewed as highly sensitive. Individual privacy in health care can be compromised in a number of ways. On the one hand, privacy may be breached and data accessed inappropriately in a serious and invasive manner (e.g., electronic data breaches through hacking), yet it may also occur in seemingly benign and informal ways (e.g., patient-specific conversations in public areas of health care facilities). Additionally, while both circumstances are breaches, they may be handled and interpreted differently. Beyond the act of communication itself, it is important to consider the content and context of these exchanges. Privacy is not clear cut and simple to understand in these contexts, and it is further complicated by the fundamental necessity of information sharing in the health domain.

Ultimately, there is a need to balance information sharing and protection in health. Both are fundamentally necessary in health, but they need not be presented as dichotomous binaries. I visualize the issue, rather, as a spectrum containing a wide range of grey areas that constitute that balance, within which the needs, demands, and constraints of a huge range of actors are being addressed in various capacities. Treading the line between demands for information sharing and protection is challenging. The construction of this thesis is therefore a balancing act. On the one hand, I attempt to illustrate the importance of information sharing and use in health. On the other, I discuss the value of privacy, particularly in the health domain. Through a case study of the development and implementation of *ActionADE* (a computer-based application designed to meet informational needs about adverse drug events between care providers and across locations of care in British Columbia (BC)), I attempt to strike that balance, ensuring that the context-specific information sharing norms are upheld, particularly with a view to the expectations and preferences of patients themselves.

With a background in communication and having worked as part of a research team that is in the process of developing and implementing the *ActionADE* system, this journey began by situating the development and implementation of ICTs in heath. In Chapter 2, I present the theoretical framework from which the remainder of my writing progresses. To provide context, I include a brief overview of the dominant epistemological approaches to theorizing health technology that contributed to my understanding of health technology - notably, technology-in-practice, an approach

informed by science and technology studies (STS). I explore some of the key concepts that emerge out of this orientation, focusing on issues related to classification. I also identify the main advantages of data collection, use, and sharing in health.

In Chapter 3, I attempt to convey my journey disentangling the complex and messy field of privacy. Having little formal education on the topic, I was pointed to Helen Nissenbaum's book, *Privacy in Context* (2010). This text served as a starting point from which I explored further areas of privacy in the disciplines of law, philosophy, and ethics. I found commonality between Nissenbaum and Daniel J. Solove's extensive writing on the topic. Both Nissenbaum and Solove often challenge traditional approaches to conceptualizing privacy, which have been deemed largely flawed in the health domain. Generally, the frameworks under which we traditionally think about and construct privacy are largely inadequate in managing the unique nature of health information. As a result, in the third chapter, I present an approach to reconceptualizing privacy through the sociotechnical lens that is outlined in Chapter 2. In doing so, I highlight the importance of contextuality, and I pose the question of why privacy actually matters, presenting a case for the protection of information.

I applied this context-specific, sociotechnical lens to reconceptualizing privacy in the *ActionADE* research project, a project I have worked on as a research assistant since beginning my Master's program in 2014. In Chapter 4, I describe this case and the methods used to study the issue of privacy and information sharing in the context of *ActionADE*. In this chapter, I describe the use of Adele E. Clarke's (2005) situational analysis, a theory/methods approach. A particular aspect of Clarke's work that I had been drawn to is the notion of implicated actors, individuals for whom assumptions are made regarding preferences and attitudes in a given situation. In the realm of data privacy and sharing, patients are highly implicated, having little say in system design and policy setting. As such, the methods for this undertaking have analyzed data from focus groups among patients on the topic of data privacy. I also focus on the broader situation, taking into account other individual and collective human and non-human actors, political elements, and discursive positions.

In Chapter 5, I present the analysis of the information sharing and privacy situation using Clarke's (2005) cartographic approaches. I use a social worlds and arenas map, situational maps, and a positional map to both analyze and visualize the

complex circumstances into which *ActionADE* will be introduced, including findings from the patient focus groups that address issues related to health data sharing and privacy quite broadly and specifically in the context of *ActionADE*. I also examine the different discursive positions that are used to discuss the relationship between information sharing and protection in health. Using these findings, I produce a series of recommendations and outline some implications that may be used to inform the design and implementation of the *ActionADE*.

In Chapter 6, I conclude by reviewing the key points and findings of this thesis. I present some of the limitations that have come to bear on the research process, and I identify avenues for future research that may be explored specifically in the *ActionADE* project, as well as in the field of health data sharing and privacy more broadly. Building on the work of the previous chapters, I argue that a balance between the need to share and protect health information may be achieved through context-specific research that seeks to understand the entire situation into which novel ICTs are to be introduced, while taking into account the perspectives of individuals to whom the information relates.

Chapter 2. ICTs in Health and Health Data

2.1. Introduction: The Proliferation of Technologies in Health and Health Data

The proliferation of technologies has played a significant role in the advancement of health care delivery and outcomes. A great deal of literature in a number of disciplines has been devoted to the study of health technologies and health informatics. Since the 1960s, the rise of medical records and other ICTs in health has been coupled with the push toward rationalization, standardization, and integration (Berg, 2004; Kaplan, 1995; Timmermans & Berg, 2003a). These trends persist today, particularly in the Canadian context. The adoption and implementation of electronic medical records (EMRs) remains at the top of political and organizational agendas, while the interoperability of health systems remains elusive both within and across the provinces (Zinszer, Tamblyn, Bates, & Buckeridge, 2013). The rationalization of medicine has contributed to the turn toward evidence-based medicine (Berg, 2004). New areas of study in relation to health ICTs are continuously emerging. In sum, the nature of the medical technology landscape is highly complex, merging the social and the technical.

A broad range of devices, tools, and treatments are combined in a multitude of ways to maintain the delivery of effective and efficient health care. The alliance of human actors (e.g., doctors, nurses, etc.) and non-human technical artefacts (e.g., paper- and computer-based records, medical devices, etc.) perform widely variable, context-specific roles. A commonality among many of these systems is the capacity to communicate, enabling faster and easier flows of information. The extent to which information sharing is made possible with the aid of these novel ICTs is unprecedented, and along with the introduction of new possibilities (such as enhanced data availability for research), new issues and questions arise. Concerns related to data ownership, patient privacy, the ethics of genomic research, and many more, have begun to elicit debate among academia, policymakers, and the general public. The study of this phenomenon demands a robust and comprehensive theoretical and methodological framework.

The following chapter will examine various approaches to theorizing ICTs, both broadly and specifically within the health domain. Through this discussion, I will identify the theoretical orientation of this research project. I will then continue by situating health

data and broader trends in big data through the lens of STS, which has provided the main theoretical orientation for my work. In doing so, I identify advantages to information collection, use, and sharing in health, both in the immediate clinical encounter and beyond.

2.2. Theorizing ICTs in Health

Like all technologies, there are a number of perspectives that have informed the study of the relationship between health technologies and society. In a study of sociological literature on medical technologies, Stefan Timmermans and Marc Berg (2003b) identify three broad theoretical camps into which the literature falls: technological determinism, social essentialism, and technology-in-practice. This categorization has been echoed by Steve Matthewman (2011), albeit in different terms, referring to each wave as anti-humanist, humanist, and post-humanist. These three positions will be explored very briefly below, approached through the lens of interpretation offered by Timmermans and Berg, while drawing from Matthewman and other sources. It is important to note that literature concerned with the sociology of medicine is extensive and thorough. The following is therefore intended only to summarize the literature briefly, without being exceedingly reductive, and serve as a foundation for the remainder of this thesis.

2.2.1. Technological Determinism

In medical sociology, and in the study of technologies more broadly, early discourse tended to take a definitively deterministic orientation. Technologically deterministic discourse privileges the role of technologies in affecting social change and political power (Matthewman, 2011; Timmermans & Berg, 2003b). This approach tends to focus on controversial technologies and presents the effects of these technologies as harmful (Timmermans & Berg, 2003b). According to Timmermans and Berg (2003b), “technological determinism as it presents itself in medical sociology is usually not about analysing technology; it is ultimately about constructing a symbolic case against medical hegemony” (p. 100). This symbolic case tends to posit that technological change will inevitably disrupt the status quo. The product of this problematic focus is an analytically reductive argument that relies too heavily on simple and broad cause-and-effect

relationships, thereby limiting the value of its analytical properties (Timmermans & Berg, 2003b). For example, some advocates for dying with dignity have argued that resuscitation techniques, technologies for artificial ventilation, and other life-saving medical technologies are a symbol of the medicalization of death, unduly extending the death process for individuals with terminal illnesses and removing their autonomy at end of life (Timmermans & Berg, 2003b). By placing exclusive blame on technologies, this argument fails to identify any broader socio-political elements and contextual factors that influenced the development and adoption of these technologies and practices. Timmermans and Berg (2003b) also demonstrate that the deterministic rhetoric may be employed to argue the opposite: that these technologies of resuscitation may be symbolically valuable because they offer advance warning of the dying process, giving loved ones and friends time to come to terms with death. Therefore, deterministic arguments are generally reductive and unproductive, simplifying away complex sociotechnical realities.

2.2.2. Social Essentialism

The social essentialist approach presents a radical shift from the previous focus on controversial technologies, illuminating instead the role of the social in the construction of technologies and taking a distinctly humanist approach (Matthewman, 2011; Timmermans & Berg, 2003b). This perspective rests upon the inherent neutrality of technologies, which are interpreted and assigned meaning through social forces (Timmermans & Berg, 2003b). In this regard, technologies achieve meaning solely through the priorities, needs, wants, and values that social actors imbue into them. This approach has also attracted some criticism, however, largely due to the overwhelming focus on the social, which results in a neglect of the technological and a failure to illuminate the symbiotic nature of the relationship between technology and society (Matthewman, 2011; Timmermans & Berg, 2003b). An example of this in the literature is a study that examined the role of electrocardiographs in reassuring patients, mediating relationships between care providers, and fortifying authoritative mechanisms over patients, suggesting that this technology attained meaning only through its use by human actors (Daly, 1989; Timmermans & Berg, 2003b).

One approach that has emerged out of social essentialism, termed the social construction of technologies (SCOT), attempts to bridge this gap. SCOT, rooted in STS,

undertakes analysis from institutional, social, economic, and political perspectives (Matthewman, 2011). Unlike technological determinism and social essentialism, SCOT argues that the progress of technologies is both contingent and multi-directional, emerging out of complex and negotiated processes that inform invention and the non-linear nature of innovation (Matthewman, 2011). As a result, contemporary interpretations of social essentialism present an illustration of the relationship between technology and society in more egalitarian terms, while maintaining an allegiance to the historical emphasis on the social.

2.2.3. Technology-in-Practice and STS

Since the 1990s, many medical sociologists have adopted a more balanced approach to theorizing and understanding the relationship between technology and society, which also draws from STS. This shift represents the third dominant approach to studying medical technologies, termed technology-in-practice. Technology-in-practice, and STS more broadly, consider technology and society in terms of the actors who have a stake in the development, implementation, adoption, resistance, success, and/or failure of technologies (Timmermans & Berg, 2003b). This analysis includes both human and non-human actors, as well as the contextual factors that emerge out of these relationships, including cultural norms, political landscapes, the availability of funding, and so forth (Timmermans & Berg, 2003b). The context is being continually regenerated as an outcome of the relationships between human and non-human actors and broader sociopolitical and organizational circumstances (Aarts, Callen, Colera, & Westbrook, 2010; Greenhalgh & Stones, 2010). Like social essentialism, technology-in-practice also acknowledges the importance of values in technological development. As a result, ICTs in health may be described and presented as actors that both produce and are a product of society. A key component of this approach is the study of technologies in action, situating their development and use either ethnographically or historically (Suchman, 2006; Timmermans & Berg, 2003b). This represents a rejection of the power ascribed to technology in deterministic terms, while also avoiding the neutrality of technologies in social essentialism (Timmermans & Berg, 2003b).

At a fundamental level, technology-in-practice and STS intend to respond to the question of what technologies actually do, situating them practically within the broader environment (Suchman, 2006; Timmermans & Berg, 2003b). The failure to situate

technologies within existing sociotechnical contexts prohibits the new technologies from achieving their full potential, particularly in the clinical environment (Balka & Kahnamoui, 2004). Furthermore, technological shortcomings result in scenarios wherein end-users develop informal workarounds to adapt the technology to their needs, which may compromise the safety of patients (Balka & Kahnamoui, 2004; Taylor, Groleau, Heaton, & Van Every, 2001). What has therefore emerged as a central tenet in ICT design in health (and in other sectors) out of this robust theoretical framework is the focus on end-user involvement. It has been argued that by including end-users in technological development, there are likely to be fewer instances of inadequate integration of ICTs, greater likelihood of meeting the informational needs of users, and so on (Taylor, Groleau, Heaton, & Van Every, 2001). The complete elimination of unintended consequences is impossible, but through the use of appropriate methodologies, systems designers are better equipped to manage and prepare for them.

Overall, STS-based perspectives and technology-in-practice acknowledge that ICTs reconfigure relations, roles, and responsibilities, produce unanticipated effects, and introduce new dilemmas and problems. Although this theoretical perspective is that which most researchers adhere to in the contemporary context, there is tendency toward the vague (albeit valuable) conclusion that the implications of ICTs introduce both possibilities and problems (Hanseth & Monteiro, 1997). Although there are many more nuanced areas of research and methodological consideration than is possible within the scope of this thesis, a selection of STS concepts will be explored below, particularly as they relate to health data.

2.3. Health Data & Big Data in Health

The proliferation of ICTs in health, and the resultant health-related data and indicators, reflect broader trends in big data that prevail in other sectors. Although the notion of big data is a widely discussed and debated facet of the contemporary sociotechnical landscape, it is defined broadly and variably, often being used as a buzzword. The term itself suggests that the key characteristic of this phenomenon is its size and, as a result, that is often a central component of its definition. For example, big data has been defined in relation to the management of either large datasets or several small datasets that can be combined to produce a large amount of data (Bourne, 2014). An exclusive focus on the ‘big’ in big data, however, fails to adequately capture its

breadth and scope (Bourne, 2014; Lyon, 2015). Bourne (2014), for example, argues that big data extends beyond the data itself, encompassing the future uses of the data that have not yet been identified or articulated. Similarly, others have posited that the practices and processes surrounding the management and use of data are equally important (boyd & Crawford, 2012; Lyon, 2015). A common approach to understanding big data is according to the '4 V's': volume, velocity, variety, and veracity (Kruse, Goswamy, Raval, & Marawi, 2016). Recently, it has been suggested that the phenomenon itself may be too abstract to be contained within a singular, one-size-fits-all definition (Auffray & et al., 2016). Definitional ambiguity aside, it is clear that big data is a highly complex sociotechnical phenomenon. It exists at the intersection of volatile social, political, organizational, and technological environments, being employed in a number of key uses in health care. Data in the health sector emerges out of a variety of sources, such as genomics, electronic health records (EHRs), clinical trials, wearable devices, and patient registries or databases (Auffray & et al., 2016; Kruse, Goswamy, Raval, & Marawi, 2016). These data sources present a wealth of opportunities and challenges, which will be explored below.

2.3.1. Informational Continuity of Care

Data collection, sharing, and use have clear and obvious benefits in health care, particularly during the clinical encounter. At the individual level, effective communication is a fundamental component of informational continuity of care, which involves the use of patients' medical histories, in addition to preferences and personal circumstances to facilitate the delivery of quality care (Haggerty, et al., 2003; Price & Lau, 2013). Continuity of care is distinguished by the temporality of care and the focus on the individual (Haggerty, et al., 2003). Informational continuity of care represents one facet of the continuity of care matrix. Beyond the informational component, continuity of care is maintained through management continuity (the management of the patient's health condition that is responsive to changing needs) and relational continuity (which is characterized by an ongoing relationship between care provider and patient) (Haggerty, et al., 2003). Informational continuity of care is a key component of the provision of care, especially for complex patients who require multidisciplinary care teams that often work independently from one another. Therefore, informational continuity of care seeks to encompass both temporal and spatial aspects of care.

A lack of interoperability represents a significant challenge for the success of informational continuity of care (Canada Health Infoway, 2014). The fragmented health system in Canada is characterized by communication systems that operate in silos due, at least in part, to a lack of coherent national (or provincial) strategy for EMRs. Rather than achieving continuity, this situation points to a reality of informational discontinuity of care, the consequences of which are many. Care providers must piece together disparate, incomplete medical histories from a range of sources to form an understanding of the patient's current circumstances and care needs. In the absence of effective information sharing, patients are often tasked with filling gaps, which becomes increasingly difficult as individuals visit multiple care providers to manage complex conditions and health statuses.

2.3.2. The Secondary Uses of Health Data

Beyond the immediate advantages of data sharing through ICTs in the clinical encounter and throughout a patient's care trajectory, the usability and value of health data continues. The secondary uses of health data refer to the use of data beyond the original reason for its collection in order to support research, policy planning, public health surveillance, quality improvement, and commercial activities (CIHI, 2013; Grande, Mitra, Shah, Wan, & Asch, 2013; Safran, et al., 2007; Tolar & Balka, 2012; Whetton, 2013). A report completed by the Canadian Institutes of Health Information (CIHI) (2013) argues that the secondary uses of health data contribute to the strengthening of the health care system in a number of ways. In addition to responding to demands for more, better care with fewer resources, secondary uses also add value to existing investments in electronic health infrastructure (CIHI, 2013).

Public health surveillance is a core component of the secondary uses of health data. Data collection for disease surveillance has been an important aspect of western health systems since the end of the 19th century (Mariner, 2007). Originally, disease surveillance was established to permit the tracking of diseases, such as smallpox, and thereby limit their spread through the creation of geographic quarantine areas (Mariner, 2007). The scope of public health surveillance has since expanded, encompassing such disease states as cancer, congenital anomalies, and adverse drug reactions. Modern disease surveillance collects data and monitors distribution, incidence, causality, and

treatment interventions, thereby enabling better health outcomes at the population level, while expanding the scope and capacity of health research (Mariner, 2007).

2.4. Standards & Classification

Public health surveillance and other secondary uses of health data are considered some of the key opportunities for big data in health in the future. The immediate and future usability of data relies in part on the structure of the data and standardization across data sources (Kruse, Goswamy, Raval, & Marawi, 2016; Tolar & Balka, 2012). Beyond simply ease of use, a successful data standards and classification system has the capacity to enable coordination across space and time, establish benchmarks for success, and so forth. While establishing data fields is a fundamental component in the design of health ICTs, it is highly politicized and demands the negotiation of significant sociotechnical complexity (Bowker & Star, 1999). This is not always successful and therefore demands study through a sociotechnical lens. Indeed, not all attempts at classification schemas produce standardization, but every standard rests upon a classification scheme (Bowker & Star, 1999). Yet as standardization remains a part of the quest toward rationalizing medicine, ensuring the appropriate classification scheme for optimized data collection is paramount (Timmermans & Berg, 2003a). These issues will be explored in further detail below.

The current emphasis on standardization began in the 1980s, coinciding with the rise of patient-specific EMRs, as well as the professionalization of medicine and institutionalization of health (Timmermans & Berg, 2003a). Standards became an important aspect of record-keeping, accreditation, and the construction of medicine as a science, while also contributing to the re-ordering of work in health by creating new careers and demand for organizational and architectural restructuring (Timmermans & Berg, 2003a). Classification is an important component of standardization. Like standardization, classification is inherently political, serving to segment the world spatially and/or temporally (Bowker & Star, 1999; Taylor, Groleau, Heaton, & Van Every, 2001). The establishment of classificatory principles are also subject to negotiations that reflect relevant moral and ethical issues (Bowker & Star, 1999). Advocates for standardization and classification argue that it will lead to enhanced communication and collaboration, pushing the art of medicine toward a self-regulating, exact science (Timmermans & Berg, 2003a). Standards, however, have not always been embraced

openly and willingly. They may be perceived to contradict the individuality inherent to medicine and diminish the patient-centeredness of treatment (Timmermans & Berg, 2003a). Furthermore, it has been illustrated that the highly complex task of establishing standards of communication is often underestimated and that the advantages tend to be overstated (Hanseth & Monteiro, 1997; Timmermans & Epstein, 2010).

Different types of standards bring about different forms of regulation and control. Four varieties of standards have been identified: design standards, terminological standards, performance standards, and procedural standards (Timmermans & Berg, 2003a; Timmermans & Epstein, 2010). Design standards become an important component of user-friendliness and interoperability of EMRs; terminological standards dictate the language of diagnosis and prognosis; performance standards guide the accreditation of hospitals and are important to quality; and procedural standards define given care paths through clinical practice guidelines (Timmermans & Epstein, 2010). This list is not exhaustive, and there is rarely mutual exclusivity in the categories. In any given technical intervention, a combination of these standards will be employed and taken into consideration. There are several dimensions of standards that have also been identified by Bowker and Star (1999): they produce objects through a set of rules that have been negotiated and agreed upon; they persist across space and time; they enable interoperability; they are legally enforced; they are difficult to change; and, they are not always a representation of the best or most efficient standard.

The establishment of standards is not straightforward. Standardization is achieved through a series of negotiations and compromises (Berg, 2004). Different stakeholders, including political entities, system designers, and end-users have different goals that they wish to imbue into systems, including those related to standards and classification. As a result, values and ethics play a role in the standards and classificatory principles that guide data input and output. This, in turn, establishes boundaries that privilege some and exclude others (Bowker & Star, 1999). These outcomes are often a reflection of the goals and needs of those in power. They require significant resources to implement and become agreed upon (Timmermans & Epstein, 2010). Standards, however, are rarely considered beyond these initial phases of negotiations. They tend to fade from visibility, become difficult to change, and transform into infrastructure (Bowker & Star, 1999; Timmermans & Epstein, 2010). That is, however, until the infrastructure breaks down, wherein the components become visible

again (Bowker & Star, 1999). Breakdown in infrastructure often emerges as a result of the conflicting and simultaneous need for both technical flexibility and standardization (Bowker & Star, 1999; Star & Ruhleder, 1996). This is a reflection of the desire and need to respond to both local and global requirements and demands. Star and Ruhleder (1996) suggest that the resolution of this tension is an important component in the establishment of infrastructure. Yet social needs are constantly changing, emerging and evolving through time and space, reflecting the dynamic nature of the health sector and the continual negotiations that are required as part of systems development.

The politicized negotiations that inform data inputs have profound effects on data outputs. Classification has the capacity to discursively construct and define identities, thereby producing political and social consequences (Balka & Star, 2015; Taylor, Groleau, Heaton, & Van Every, 2001). Of importance, it must be emphasized that EMRs and the classificatory principles that inform them are not mirrors of the individual. Rather, they are tools that mediate the patient encounter and serve as the histories and memories of individuals in partial views (Balka & Star, 2015; Berg, 2004). Furthermore, in light of the mutual exclusivity that characterizes many classification systems, we must consider the social and political consequences of classification, with particular attention to those who do not fit or those who are misclassified (Bowker & Star, 1999). One well-known schema of standards is the International Statistical Classification of Diseases and Related Health Problems (10th Revision) (ICD-10), published by the World Health Organization. ICD codes are used internationally to classify diseases for clinical, public health, and research purposes. The ICD only classifies diseases that are considered statistically significant, and those that constitute the biomedical interpretation of disease that informs the classification (Bowker & Star, 1999). The current ICD was developed over twenty years ago, which also has an effect on the manner in which it classifies. For example, the discovery of new diseases and changes in the way that diseases and conditions are socially interpreted may not be reflected in the current ICD system. In advance of the introduction of the ICD-11, set to be released in 2018, the Working Group on Sexual Disorders and Sexual Health was convened to make recommendations for the upcoming revision related to the classification of sexuality and gender identity in the ICD-10, which are exemplar of some of the consequences of classification (Reed, et al., 2016). Of note, the current ICD classifies transgender identity as a mental disorder. The authors suggest that this exacerbates existing stigma that is faced by these populations,

which has “contributed to precarious legal status, human rights violations, and barriers to appropriate health care in this population” (Reed, et al., 2016, p. 206). Furthermore, classification as a mental disorder suggests that transgender individuals need to seek treatment in the realm of psychiatry, which contributes to the limited health services that they may seek elsewhere (Reed, et al., 2016). The authors have therefore argued that transgenderism remain within the ICD in order to ensure access to services is not compromised beyond the current environment, but to move the classification into a newly proposed chapter, titled Conditions Related to Sexual Health in ICD-11 (Reed, et al., 2016).

The barriers for those who experience the consequences of classification, misclassification, and othering are significant (Bowker & Star, 1999). As noted by Balka and Star (2015), “at the same time that standardized, single indicators...both compose and reduce us, they simultaneously mask all the complexity of what lives in residual categories” (p. 429). These partial views and those that fall outside classification may be understood as shadow bodies (Balka & Star, 2015). Shadow bodies are representations and abstractions of human beings, bringing to light certain aspects of the self and hiding others (Balka & Star, 2015). That which is hidden and that which is exposed is a reflection of the classificatory principles and data standards enshrined into the underlying infrastructure, based on the preferences, values, and informational needs of its creators (Balka & Star, 2015; Bowker & Star, 1999). The resultant records create a snapshot of the individual at a particular place and time, providing certain information as required, but concealing other things: “Our lived experiences exist in the shadows, sometimes visible, sometimes not, depending upon how the light falls” (Balka & Star, 2015, p. 429). Although deeply entrenched in technological requirements and constraints, shadow bodies are a product of social and political realities and may produce significant personal and political consequences.

2.5. Conclusion

This chapter has presented the dominant approaches used to theorize the relationship between ICTs and society. In doing so, I have positioned the remainder of this thesis in a sociotechnical lens, informed by STS and technology-in-practice. I have identified the value of this lens in studying various aspects of health data and highlighted key issues related to standards and classification. The personal and political

consequences of classification and standardization in health are a facet of other challenges related to data security and privacy. As with many other sectors in which ICTs and data proliferate, the value of privacy is one that is highly contested. It is situated within broader political, organizational, and social contexts and needs. When privacy in ICTs and in health data are debated, what exactly is being discussed? Why is it something that is considered valuable, and how can it be studied in a balanced way that avoids the rhetorical traps of technological determinism and social essentialism? There is a strong need to unpack the concept of privacy in relation to health data to understand how it is operationalized in sociotechnical and political systems. This will be addressed in the following chapter.

Chapter 3. Approaching Privacy

3.1. Introduction

Historically, confidentiality has been a key component of the practice of medicine and a defining trait of the patient-clinician relationship. Dating to approximately the fourth century BCE, physicians across vast geographic regions have been bound by the eighth principle of the Hippocratic Oath, sworn to maintain the confidentiality of patient information (Nissenbaum, 2010). Contemporary organizational and technological changes in the field of medicine have challenged the Hippocratic Oath's capacity to protect patient information (Nissenbaum, 2010). Various privacy oriented measures have thus been introduced to manage the range of human and non-human actors that encounter and interact with patient information across space and time.

Managing expectations of privacy are achieved through both the formal conditions of privacy, mainly in the form of legislation, and the physical and technical conditions of privacy, which can include technical specifications and modifications to the built environment (Reiman, 1995). The legislative environment in Canada, which will be discussed at length in Chapter 5, consists of a mix of federal and provincial laws that apply in varying contexts. Some provinces have legislation that is specific to health information, such as Alberta and Saskatchewan, but others (including BC) treat health information as the same as other personal information. The adequacy of the legislative regimes is often called into question by privacy experts. Daniel Therrien, the current Privacy Commissioner of Canada responsible for independent oversight of privacy rights in Canada, has criticized the current legislative regimes as failing to maintain pace with technological changes and as becoming increasingly irrelevant (Boutilier, 2016). Regular reviews of federal legislation have also elicited complaints and critiques from prominent privacy scholars. In a recent review by the Standing Committee on Access to Information, Privacy and Ethics (2017), the current Canada Research Chair in Ethics, Law and Technology, Ian Kerr, raised concerns about transparency and consent in the current legislation. Director of the Centre de recherche en droit public, Vincent Gautrais, also testified, adding to the discussion on the effectiveness of consent (Standing Committee on Access to Information, Privacy and Ethics, 2017). Anxieties related to national security have also been criticized for eroding the privacy of individuals,

particularly with the recent passage of a controversial anti-terrorism law in Canada, titled Bill C-51. This legislation strengthened police power through a number of measures, such as increased information sharing between governmental departments, including Health Canada. Although the passage of Bill C-51 elicited protests and public outcry, as well as an electoral promise from the current federal government to repeal parts of the law, it is still a problematic facet of the current Canadian privacy landscape (Braga, 2017).

The need to protect data privacy in health is a significant challenge, as it requires managing the expectations of information sharing that were highlighted in the previous chapter, and the need for privacy with regard to highly sensitive personal health information. Other privacy critics offer context for broad privacy issues in Canada, but the unique nature of health information and the federalist structure of health delivery demands a context-specific analysis. This chapter will set the stage for an analysis of the need to balance information sharing and protection by unpacking the meaning of privacy and the implications of poor privacy protections. I begin by broadly discussing the major approaches to conceptualizing privacy. I describe how traditional conceptualizations are incompatible with the complex nature of health information sharing. I then identify approaches to reconceptualizing privacy within a sociotechnical lens, applying the theoretical constructs that were identified in the previous chapter. I conclude by presenting a case for the protection of privacy through an examination of different information-based harms that emerge in contexts with inadequate privacy provisions.

3.2. Conceptualizing Privacy

Privacy is a complex and messy topic. It is beyond my current capacity to address the breadth and depth of scholarly work on the topic of privacy. Therefore, the following section presents merely an overview, identifying and discussing the dominant approaches to conceptualizing privacy, particularly as they relate to personal health information. Rather than provide an exhaustive account, I intend to set the stage for the practical applications that concern the flow of personal health information, which will follow.

Conceptualizing privacy often begins with defining the meaning of privacy, an activity that has been fraught with ambiguity (Moore, 2008; Viseu, 2004). To understand

this variability, Nissenbaum (2010) categorizes interpretations of privacy across three dimensions: normative versus descriptive accounts; definitions provided in terms of access versus those in terms of control; and, those that explore the normative strength of privacy due to its ability to advance other values versus those that delineate privacy as something that protects a distinctively private realm. These dimensions will be explored below.

3.2.1. Normative versus Descriptive Definitions of Privacy

Whether privacy is constructed descriptively or normatively has a strong impact on its application. Normative definitions of privacy center upon the notion of privacy as a value, giving it moral legitimacy and positioning it as something that is fundamentally 'good' and worthy of legal protection (Nissenbaum, 2010; Zimmer, 2015). Descriptive definitions, on the other hand, are considered neutral, describing "a state or condition where privacy obtains." (Moore, 2008, pp. 412-3) This is to say that privacy is a state of being, without arguing that it is inherently good and worthy of protection. Furthermore, a descriptive definition does not suggest that any increase or decrease in privacy is inherently good or bad. Approaching privacy from this perspective avoids subscription to such terms as 'violation' or 'breach', by positioning these effects more neutrally through the use of terms like 'reduction' or 'diminishment' (Nissenbaum, 2010). Perceptions toward privacy are thus discursively constructed through the use of either normative or descriptive accounts.

3.2.2. Access versus Control (versus Other Interpretations)

Another definitional dichotomy that is characteristic of traditional interpretations of privacy are those that emphasize access and those that emphasize control, in addition to other interpretations that often touch upon aspects of access and control.

Privacy as Control

Understanding privacy as the capacity to control one's personal information tends to frame it in terms of ownership (Solove, 2001; Solove, 2002). Prominent legal scholars Alan Westin and Charles Fried were essential to the advancement of the notion of control in relation to information privacy. In Westin's *Privacy and Freedom* (1967), he defines privacy as: "the claim of individuals, groups, or institutions to determine for

themselves when, how, and to what extent information about them is communicated to others." (p. 7). Similarly, Fried (1968) defines privacy as: "control over knowledge about oneself." (p. 483). This narrative has thus been a dominant approach to privacy, having shaped policy and law in much of Canada and the United States (US), including as it is applied to personal health information.

The interpretation of privacy as control has faced criticism. It has been argued that it is too generalized to reflect the idiosyncratic nature of privacy in different contexts (Nissenbaum, 2010). Solove (2002) argues that it is all at once too vague (by failing to define which kinds of information individuals have control over), too broad (by failing to operationalize the term control), and too narrow (by focusing exclusively on informational concerns and individual choice). This conception also fails to take into account the social norms that govern the disclosure of certain information, regardless of personal autonomy (Mariner, 2007; Reiman, 1995; Solove, 2002). Consider, for example, the case of sexual offenders, whose status is legally required to be disclosed for the safety and security of the public, and therefore is out of the control of the individual. In health, the notion of privacy as control would suggest that patients have control over the trajectory of their personal health information, but this is largely not the case. The extent to which health information is shared across a diversity of actors challenges the notion that this information can truly be owned.

Privacy as Access

Control is a valuable conception of privacy under certain circumstances, but considering the flow of information in terms of degrees of access permits a more detailed account of the conditions that surround privacy (Nissenbaum, 2010). Understanding privacy along the lines of access positions it as the capacity to limit others' access to information about oneself, access to one's physical self, and access to paying attention to oneself (Gavison, 1980). Although this position has been widely advanced, definitional ambiguity emerges in consideration of which matters should be considered private, what levels of access are ascribed to that private information, and as a result, what would warrant a violation (Solove, 2002). In health care, this ambiguity may be especially problematic due to the breadth and scope of information that is collected, accessed, and used in a wide range of settings.

Other Interpretations

Solove (2002) identifies four additional interpretive lenses beyond access and control that can aid in understanding privacy, which will be discussed in brief below. There is significant overlap among these concepts, and many touch upon aspects of control and access as well. These additional conceptualizations are: (i) the right to be let alone; (ii) secrecy; (iii) personhood; and, (iv) intimacy.

The right to be let alone is largely based on Warren and Brandeis' (1890) seminal text, *The Right to Privacy*. Written during a time of significant technological change, Warren and Brandeis urged policymakers and lawyers to enshrine the right to privacy within the American justice system due to the failure of existing policies to protect against the psychological harm introduced by novel technologies (Nissenbaum, 2010; Solove, 2002). The phrase 'the right to be let alone' was advanced following Brandeis' publication of a dissent against the *Olmstead v. United States* case, wherein the constitutionality of wiretapping was being contested (Solove, 2002). It is predicated on the idea of the existence of a distinctly private realm that is worthy of protection, which will be explored more in section 3.2.3. Solove (2002) notes, however, that this conceptualization fails to situate privacy relative to other social values and has been widely critiqued for failing to advance privacy beyond the identification of gaps in the law torts, which protect individuals from suffering harm due to a wrongful act. Nevertheless, Warren and Brandeis' text has served as the foundation for much of the privacy law in the United States and Canada throughout the twentieth century (Nissenbaum, 2010).

When privacy is presented as secrecy, it denotes the ability to conceal information and prevent it from being disclosed publicly. Privacy as secrecy is a subset of the access narrative, as it suggests that the individual has agency to limit the extent to which others have access to personal facts or information on them (Solove, 2002). Being a subset, however, is indicative of the narrowness of this argument. In reality, not all that is private is secret and vice versa (Solove, 2002). For example, one's political affiliation may be viewed as private, but not necessarily a secret. On the other hand, for instance, court proceedings that are under publication ban are to be kept secret, but are not by and large private.

Privacy as personhood is often used in conjunction with the other theories discussed above. It generally positions privacy as a way to protect the integrity of the

individual, so that one may have the autonomy to be their true selves, a conceptualization that has been supported by legal institutions as well (Solove, 2002). Reiman (1976) defends this thesis, arguing that privacy is a prerequisite for the establishment of the self and essential to the maintenance of this sense of personhood. This corresponds to the conceptualization of privacy as advancing other values, which will be discussed in the following section. Understanding privacy in terms of personhood, however, has been critiqued for poorly articulating the meaning of personhood (Solove, 2002).

Lastly, privacy may be conceptualized as intimacy. Although this too has been ambiguously defined, intimacy excels by accounting for the effect of interpersonal relationships on information sharing preferences. In this sense, privacy is contingent upon the relations one has with others, and the sharing of personal information depends on the nature of these relations. This, however, is its downfall, as information-based privacy is not exclusively contingent upon personal relations, extending to more formal encounters, including the provision of health care (Solove, 2002). As Reiman (1976) illustrates, one might share private information with a psychologist that they may refrain from sharing with a partner or friend.

3.2.3. Privacy Advancing Other Values versus Protecting a Private Realm

The final dimension along which Nissenbaum (2010) places conceptualizations of privacy are from which realm privacy draws its prescriptive power. One aspect of this dimension is the suggestion that privacy is essential toward the advancement and maintenance of other values that are perceived to be fundamental aspects of liberal democratic societies. These values include autonomy, creativity, mental health, and so forth (Gavison, 1980). Privacy is therefore important for individuals, their relationships, and their existence within society (Nissenbaum, 2010). This perspective is useful when considering the effects of sociotechnical systems in relation to other values, offering an argument for the protection of privacy (Nissenbaum, 2010; Reiman, 1995).

Others have conceptualized a distinct private realm that employs privacy as a way to protect and maintain its sanctity. This is generally understood as the public/private dichotomy, whereby that which is in the public sphere does not warrant a

need for privacy. There are three dimensions along which the public/private dichotomy is applied, which are the actors, often framed as governments in contrast to private citizens, spatial realms, and information (Nissenbaum, 2010). The distinction generally rests upon the interpretation of intimacy, described above, whereby interpersonal relationships are central to determining acceptable access (Nissenbaum, 2010). The public/private distinction is often a foundation for legal interpretations of privacy, but it largely fails to account for the fluidity and ambiguity that is characteristic of public and private realms, as well as the degrees of access based on variance in interpersonal relationships (Nissenbaum, 2010).

3.2.4. Conclusion: Mapping the Dimensions of Conceptualizations of Privacy

It has been widely acknowledged that understanding privacy is a complex and difficult task, made even more difficult by the multiplicity of interpretations from a range of disciplines. The discussion above has attempted to delineate the various dimensions along which traditional conceptions of privacy tend to align. These dimensions include the normative or neutral conceptions of privacy, privacy as access, control, or otherwise, and privacy as a means to advance other values or an end in and of itself. Oftentimes, a definition of privacy will touch upon a number of these dimensions, as well as multiple aspects within one dimension. There is clearly no one-size-fits-all definition of privacy and many of these conceptions have significant limitations, yet they have still come to influence the legislative regimes that formally govern privacy. In the following section, I will argue that many of these conceptualizations are particularly limited in the context of managing the privacy of personal health information. Hence, I propose a practical approach to understanding privacy in practice.

3.3. Reconceptualizing Privacy in Health

Privacy is normatively constructed as a core value in the information society and in health, but, as illustrated above, truly defining privacy is challenging. The nature of the word itself implies a highly individualistic experience, despite the fact that privacy is a highly social and political concept (Viseu, 2004). In health care, it is a vehicle for maintaining standard social expectations of informational flows across clinical encounters and the health system more broadly. On the one hand, appropriate,

accurate, and expedient information flows are a critical component of informational continuity of care and secondary uses of data, thereby contributing to public policy, planning, research, and so on. Simultaneously, however, this information is considered highly sensitive and deserving of protection. It is too often the case that traditional conceptions of privacy fail to account for this complexity, effectively reducing the issue to binaries, extremes, and absolutes. As noted by Lyon (2015): “privacy never exists in a vacuum” (p. 100). There is therefore a need to conceptualize, or reconceptualize, privacy while avoiding the rhetorical traps of universalities and homogeneities.

Solove (2002) suggests a pragmatic approach toward reconceptualizing privacy that emphasizes the contextual nature of privacy by rejecting traditional discourses and focusing instead on actual practices. Solove’s approach is responsive to social realities, permitting re-definition of privacy needs in actual practice. Similarly, Nissenbaum (2010) and Lyon (2015) have both emphasized the importance of contextuality in privacy, suggesting that regulations be sufficiently flexible to accommodate this contextuality, while also remaining necessarily firm to protect against harm. Nissenbaum proposes a framework to understand context appropriate flows of information, resulting in a reconceptualization of privacy that is responsive to the changing information privacy landscape. Titled the Contextual Integrity (CI) framework, this approach to reconceptualization asserts that social norms dictate the flow of information in different contexts, contingent upon the context, the actors, attributes of the information, and the transmission principles. Nissenbaum proposes this framework primarily as a means to understand the disruptive nature of novel technologies on privacy in a sociotechnical context. It is a robustly designed, descriptive tool and evaluative framework, and aligns well with many of the theoretical and conceptual orientations taken in this thesis, but it is not the appropriate framework for this undertaking. This framework is largely designed to evaluate and understand controversial technologies and sites of protest, such as CCTV.

Although the CI Framework proposed by Nissenbaum (2010) is valuable in many respects, my research undertaking seeks to evaluate the contextual factors that will come to bear on the design of a novel technology, not yet a site of protest or controversy. As will be illustrated in the following chapters, this research has sought to actively avoid sites of controversy in the development of a novel technology by engaging with and analyzing the actors involved. Applying Nissenbaum’s framework to this undertaking would be limited. I would not be able to respond to the question of where the

technology diverges from or defies existing informational norms because it is through this research that I seek to mitigate these issues at the outset, in an attempt to achieve a balance in the need for information flows and privacy. Instead, I argue that reconceptualizing privacy in these terms may be operationalized through an approach informed by STS. As discussed in the previous chapter, STS is a valuable lens for exploring the relationship between technology and society. In keeping with this perspective, I maintain that privacy is a fundamentally sociotechnical concept, particularly in relation to the contemporary health informatics landscape. It is embedded in sociotechnical and political systems both materially (e.g., through technical design and specifications) and symbolically (e.g., through legislation and data standards). Seeking balance between the need to protect and share information would thus require an exploration of situational specificities that come to bear on ICTs and information flows under different circumstances. STS is a valuable lens because it emphasizes the contextualities, situatedness, and heterogeneities of sociotechnical realities, demonstrating significant overlap with the recommendations identified above by Solove (2002), Nissenbaum (2010), and Lyon (2015).

I propose an approach to the practical application of these theoretical underpinnings by drawing from Clarke's (2005) situational mapping strategy, described in greater detail in the following chapter. In sum, situational maps enable a thorough analysis of the situation into which new and different informational flows are introduced, thereby making visible or accounting for effects of different contexts on privacy. Indeed, for Clarke, the unit of analysis itself is the situation, including all the narrative and historical discourses of the situation. Clarke's extension of grounded theory to reflect postmodern thought is also fitting, as it acknowledges the existence of multiple truths, supporting the notion that not one single interpretation of privacy may be inherently right or wrong. This interpretation permits a shift away from assumptions and homogeneities that traditionally inform privacy-related legislative regimes and design principles that are too often deemed inadequate. Another key facet of STS is the consideration of both human and non-human actors. This applies to privacy by enabling an examination of the technologies that mediate the flow of information in these contexts and lends itself to capturing the breadth and depth of actors involved in any sociotechnical circumstance. Under this model, privacy would thus be considered in the context of a specific technical intervention, or more broadly, to the scope of information flows in specific contexts. This

would situate the novel information flows in recognition of the goal of balancing both the need to share and disclose information in health care contexts.

As a part of this reconceptualization, I argue that understanding context-specific privacy expectations and norms may begin through the consideration of the circumstances under which privacy is absent. This is traditionally viewed as a privacy violation, but I will instead approach this discussion through a frame of reference that favours the term *information-based harm*. Through this discussion, I intend to illuminate and mitigate issues proactively and in practice, while avoiding the rhetorical traps of privacy's definitional ambiguity (Moore, 2008). This will ultimately present a case for the protection of health data. The following section will begin by identifying some of the major harms that may emerge out of the introduction of novel flows of information, mediated through ICTs. I then present the possible outcomes of information-based harms, particularly highlighting the narrative and discursive responses that tend to characterize broader public perceptions toward privacy issues in their day-to-day lives.

3.4. Identifying Information-Based Harms

In order to understand the importance of information protection, an examination of possible information-based harms is required. Evoking an understanding of the information-based harms that emerge is central to reconceptualizing privacy in a practical and constructive manner, by contextually situating privacy. This approach draws from philosopher Jeroen van den Hoven's (2001) work on the value of privacy, classifying this value across four categories: information-based harm, informational inequality, informational injustice, and encroachment on moral autonomy. Of utmost importance to this discussion, I emphasize that I am not taking a deterministic or constructivist position on information-based harms. That is to say that I acknowledge that harms do not emerge solely due to the development and introduction of novel ICTs, nor are they solely a factor of the human actors that add meaning to them. On the other hand, I suggest that information-based harms are a product of complex sociotechnical environments, whereby both human and non-human actors interact and exert agency in complex ways, thereby leading to instances of harm. The following section outlines the key areas of concern that come to bear particularly strongly on patients and personal health information. I first discuss the prominent types of information-based harms that

affect health data, focusing on breaches, secondary uses, and surveillance. I then illustrate the consequences of these harms, presenting a case for the protection of data.

3.4.1. Activities that Introduce Information-Based Harms

There are several ways in which novel flows of information mediated by ICTs generate opportunities for harm that would not otherwise exist. Solove's (2006) taxonomy of activities that threaten to violate privacy situate them along the lifecycle of information as it leaves the individual from the point of collection and leading to its use, storage, and dissemination, as well as in terms of direct physical intrusions onto the self. The categories in this taxonomy are information collection, information processing, information dissemination, and invasion. The harms are not mutually exclusive, and not all are relevant in each context. Drawing from Solove, the activities that are most relevant to this undertaking are breaches of confidentiality, aggregation and secondary uses of data, and surveillance. Through this discussion, I will illustrate that normative conceptions of information-based harms as 'privacy violations,' and the resultant outcomes of insult or reputational harm, should be viewed as less concerning than the more elusive architectural problems that emerge. Architectural problems create risk by either enhancing existing risks and/or upsetting the balance of social and institutional power (Solove, 2006).

Breaches

Privacy breaches are among the most widely understood type of information-based harms. The Office of the Information and Privacy Commissioner for British Columbia (OIPCBC), which provides independent oversight of information and privacy legislation in BC, defines a breach as: "any unauthorized access to personal information, or the unauthorized collection, use, disclosure or disposal of personal information," (Denham, 2015, p. 4) whereby the term 'unauthorized' denotes any violation of the terms outlined in BC's privacy legislation. Due to inconsistent legal definitions and interpretations of data use and sharing across jurisdictions, however, it may be difficult to ascertain what would and would not constitute a breach, in addition to which data uses may or may not be considered acceptable (Council of Canadian Academies, 2015; Rivkin-Haas, 2011; Viseu, 2004).

Furthermore, not all breaches are created equal. The severity of a breach may vary, depending on the type. Different types of breaches include accidental disclosure, insider curiosity, data breach by an insider for personal gain, data breach by an outsider with physical intrusion, and unauthorized intrusion of the network system (Appari & Johnson, 2010). Severity and incidence are often inversely correlated; while many may fear the cyber attacker or hacker that maliciously accesses one's information, most breaches are undertaken by those with legitimate access to the data (BC Medical Association, 2009; Council of Canadian Academies, 2015). Indeed, one study found that 36% of instances of breaches were inadvertent misuse by insiders (Council of Canadian Academies, 2015). This is what Solove (2006) would consider a breach of confidentiality, whereby harm emerges out of the violation of the trust that is implicit in the care provider-patient relationship.

There are countless instances of data breaches in health. Large scale breaches are often reported in the news media. Recently, for example, BC's provincial medication billing and management system, PharmaNet, was the target of a breach whereby the personal information of almost 20,500 residents of the province was accessed inappropriately (McElroy, 2017). In this case, the BC government has stated that it will notify those affected (McElroy, 2017). Problematically, however, many will never know that a breach has occurred and affected their information. Of note, over the past ten years, the OIPCBC has received only 200 reports of breaches from the health authorities, which is estimated to be less than one percent of the suspected breaches that have actually occurred (Denham, 2015). Presently, breach notification is not required by hospitals or care providers (McDonald & Swain, 2016). It has, however, been recommended that mandatory breach notification be incorporated into future policy reforms (OIPCBC, 2014).

Aggregation & Secondary Uses of Health Data

Other privacy violations are less straightforward than privacy breaches, often emerging as the negative facets of otherwise positive information collection and processing practices. Indeed, in health, information collection through public health surveillance and information processing through aggregation and secondary uses may be both beneficial and problematic. Aggregation is valuable for health delivery and planning, but harm emerges through the ease with which extensive data points may be

combined (Solove, 2006). Data collection and aggregation enable the secondary uses of health data, which have been described in the previous chapter.

The extension of secondary uses into tertiary and quaternary uses (and beyond) introduces concerns largely related to the notion of informed consent. While initial consent requirements in data collection generally afford individuals the knowledge of the uses of their information, tracing its path forward is much more convoluted. This is particularly problematic in an environment whereby information is collected for future uses that have not yet been determined (Lyon, 2015). Without consent, the secondary uses of health data become subject to function creep, whereby, “personal information is used for purposes not specified when the information was collected, not clearly related to the original use of the information and used without the consent of the person to whom the information relates” (Whetton, 2013, p. 234). This represents an imbalance in the normative expectations of individual and institutional control over information. Practically speaking, however, obtaining consent from each individual presents significant administrative burden, while also threatening to produce bias in data sets due to demonstrable variation in the demographic and socioeconomic composition of those who are likely or unlikely to consent (El Emam, Jonker, Arbuckle, & Malin, 2011). This presents challenges for researchers and policymakers who have sought to balance the demands of privacy and consent in practical means.

Surveillance

Broadly speaking, surveillance is the collection of information on individuals to fulfill a variety of purposes, including control, management, and protection (Lyon, 2015). Much like the secondary uses of health data, the function of surveillance in this capacity may be interpreted as both harmful and beneficial, depending upon both the context of surveillance and the perceptions of the individual.

In one sense, surveillance has been discursively constructed as government encroachment upon the lives of individual citizens (Nissenbaum, 2010). In these contexts, privacy represents a barrier between citizens and government, minimizing government intrusion in the name of liberty and autonomy (Nissenbaum, 2010). This is a particularly salient perspective in the post-9/11 digital era that is characterized by state sanctioned surveillance, most notably in the context of the US National Security Agency (NSA). Indeed, there has since been a resurgence of dystopian discourse associated

with government surveillance. Drawing from Foucault's (1975) notion of the disciplinary society, contemporary scholars have argued that the accumulation and aggregation of surveillance data enables a form of panopticism that has the capacity to render any individual visible from invisible eyes (Reiman, 1995). This sets an unprecedented standard, enabling the creation of highly detailed portraits of any individual's life (Reiman, 1995). Furthermore, surveillance data collection is amplified through device tracking and sophisticated aggregatory methods, unleashing the capacity of the disciplinary society to extend beyond the spatial confines that characterized Foucault's panopticism (Lyon, 2015). The mass acceptance and internalization of surveillance is a condition of modernity, whereby the tools that enable surveillance are built into everyday technologies (Lyon, 2015).

Interestingly, however, this discourse is largely absent in the context of health surveillance. It is more often the case that surveillance in health is presented as positive, keeping with the discursive argument that positions the value of information sharing in the interest of the greater good above that of individual privacy. Indeed, public health surveillance has produced demonstrable benefits in the past. For example, during the international outbreak of severe acute respiratory syndrome, commonly known as SARS, in 2003, public health surveillance was a key component of cluster identification, tracking the epidemic, and completing the feedback loop from government to the public and health care providers (Schrag & et al., 2004). The SARS epidemic was also a catalyst for the creation of the Public Health Agency of Canada (PHAC), which is responsible for the surveillance of many acute and chronic illnesses (PHAC, 2008). In contrast to the generally negative public sentiment toward surveillance in contexts outside of health care, there are still calls for strengthened and enhanced surveillance in health today (for example, see Smolina, Persaud & Morgan, 2016, on the need for strong prescription drug surveillance).

The positive outcomes of surveillance in health, however, do not exempt it from a critical voice. In fact, not all public health surveillance has yielded universal support. A well-documented case is the introduction of surveillance methods to address the HIV/AIDS epidemic, which brought about a sense of fear among those affected, largely due to the social stigma associated with the disease and a culture of homophobia (Fairchild & Bayer, 2016). This is illustrative of the capacity of surveillance to undermine and disenfranchise population subgroups, a process known as "social sorting" (Lyon,

2015, p. 25). These are consequences that apply to information-based harms beyond simply surveillance, and will be elaborated on below.

Overall, a key difference that is central to the notion of 'surveillance' in different contexts is that public health surveillance is promoted as serving populations by permitting interventions, whereas generalized surveillance is perceived as a means of controlling populations and limiting autonomy. Through this construction, surveillance is presented as inherently good or bad. I do not believe that the ends of public health surveillance need be questioned, rather, it is the means through which this information is being collected that must be considered critically.

3.4.2. Outcomes of Information-Based Harms and Architectural Problems

Information-based harms (e.g., a data breach of electronic medical records due to inappropriate disposal of paper files) can result in a number of negative outcomes. Patients are central and often implicated actors in the context of information-based harms. The harms concern their information, but they are rarely notified when a breach has occurred, and they have little to no agency in regaining that which was lost (physically, emotionally, and otherwise) as a consequence. These consequences are typically assumed to be a direct insult or reputational harm, but there are subtler harms that must be considered.

Reiman (1995) identifies four risks that emerge for those who lack privacy due to surveillance in the informational panopticon, although I argue that they may applied to any circumstance whereby privacy norms are challenged and information-based harms are introduced. These risks are the extrinsic losses of freedom, intrinsic losses of freedom, symbolic risks, and psycho-political metamorphosis (Reiman, 1995). A fear of the consequences of having unpopular or unconventional attitudes or behaviours results in extrinsic losses of freedom, which may lead to behavioural modifications (Reiman, 1995). In this sense, privacy permits a certain degree of behavioural liberty, wherein one may act without fear of consequence or social pressure (Gavison, 1980). Intrinsic losses of freedom occur when individuals become aware of the potential to be observed and self-censor or act differently as a result (Reiman, 1995). Both extrinsic and intrinsic losses result in a reduction and denial of agency, thereby presenting a symbolic risk

whereby individuals lose their self-ownership and their capacity to withdraw from the state of visibility (Reiman, 1995). Long-term exposure to this type of symbolic risk may result in a psycho-political metamorphosis, characterized by an internalized shift in behaviours and thoughts, resulting in reduced self-esteem or self-efficacy (Ben-Zeev, Young, & Corrigan, 2010; Nissenbaum, 2010; Reiman, 1995). Even if an invasion of privacy does not result in harm or injury to the self or to one's reputation, it still affects one's self-ownership as a consequence of these four losses (Reiman, 1995).

In the health domain, both extrinsic and intrinsic losses of freedom may have a negative effect on health outcomes. Patients may choose to alter their health seeking behaviours in order to manage those risks in the absence of adequate protections from their care providers, health technologies, and legislation (Jenkins, 2004; Sankar, Moran, Merz, & Jones, 2003; Whiddett, 2006). These protective behaviours may include seeking care from another provider, paying for services out of pocket, failing to seek care, failing to provide accurate or complete information, or requesting that a provider omit details on record (Malin, El Emam, & O'Keefe, 2013). All of these behaviours may compromise the capacity of clinicians to provide informed and appropriate care.

These issues are often conceptualized and discussed in the context of individuals living with illnesses that carry stigma, such as certain mental illnesses (e.g., schizophrenia, depression, etc.) and infectious diseases (e.g., HIV/AIDS, Hepatitis C, etc.). Indeed, in the context of individuals living with stigmatized illnesses, the risks of exposure to information-based harms are severe. In extreme cases, stereotypes in this vein may lead to discrimination, particularly in the event that personal health information does not remain within the health domain, which has been identified as a form of informational injustice (van den Hoven, 2001). This may affect employment opportunities or social relationships, but may also have unexpected effects. For example, a ban that was in place from 1987 until 2010 prohibited individuals living with HIV/AIDS from entering the US (CBC News, 2010). It was reported that this discriminatory policy exposed individuals to undue harassment when trying to cross the border from Canada into the US, largely due to misinformation and misconceptions about the disease (CBC News, 2010). Simultaneously, these same individuals face life-threatening consequences for avoiding or failing to seek proper care. This is a strong example of the need to identify a balance in information sharing and protection.

It is most often the case, however, that members of the general population who do not face stigma or discrimination in their day-to-day lives fail to see the true ramifications of these losses and harms. A prominent narrative emerges in this situation: nothing to hide, nothing to fear (Solove, 2011). The nothing-to-hide argument is pervasive, often employed in response to demands for increased government surveillance (Solove, 2011). It is difficult to imagine the effects of classification on oneself when one does fall neatly within classificatory principles, representing the norm rather than the other. However, the nothing-to-hide argument is based on flawed assumptions about privacy, specifically that it is a tool to hide only bad things, aligning with the privacy as secrecy conception (Solove, 2011). There are both tangible and abstract effects of different information-based harms for the general population that deserve attention, discussed below.

Returning, for example, to the issue of breaches, there are many tangible outcomes that may emerge. Health data is not exempt from the broader commodification of data that occurs through the collection and aggregation of data from loyalty cards, mobile applications, public records, and so on. Of note, however, in some jurisdictions, concerns related to some of these practices have been raised, resulting in legislative change that limits or prohibits the merging of health data with data from loyalty cards. For example, in BC, the BC Court of Appeals (the highest court in the province) presented a ruling in 2016 that prohibited the use of loyalty programs in pharmacies, including in Shoppers Drug Mart and Safeway (Sobeys West Inc. v. College of Pharmacists of British Columbia, 2016). Health data is highly susceptible to both financial fraud and medical fraud. It has been noted that criminals use this data to engage in identity theft, purchase and resell medical equipment and pharmaceuticals, and make fraudulent insurance claims (Humer & Finkle, 2014). One expert has noted that medical information on the black market is valued at ten times that of credit card numbers (Humer & Finkle, 2014). These immediate outcomes, however, are not often considered in the context of the nothing-to-hide argument. This is largely due to the construction of the argument, which emphasizes the information collection, rather than the way that information is used, aggregated, disclosed, and managed after initial collection. Therefore, the nothing-to-hide argument is short-sighted, failing to acknowledge the reality and permanence of information collection, use, and sharing.

Lastly, I return to the concept of shadow bodies. As I had discussed in the previous chapter, shadow bodies are a sociotechnical phenomenon concerned with the construction of identities through classificatory and infrastructural elements of technologies. I argue that this is a useful lens through which information-based harms may be framed. It offers a broad scope of understanding of the ways in which technologies and classification both highlight and hide aspects of the self, whether valid or not. Some may come to find that their representations and abstractions are simply that - representations and abstractions - which may affect the way that otherwise mundane information is presented. In considering the need for data privacy and data sharing in health, the concept of shadow bodies introduces an avenue from which individuals may ask themselves whether that is how they want to be represented. The notion of privacy, then, can serve to manage this classification and misclassification, thereby protecting the autonomy and integrity of individuals, touching upon notions of personhood, access, and control, among others, while aligning with a normative conception of privacy.

3.5. Conclusion

The material I have addressed above, taken together, suggests that all possible information-based harms must be considered in context, as a whole. No privacy threat exists in isolation. Greater surveillance permits aggregation, which enables more secondary uses. As the tendrils of data grow, they introduce more opportunities for breaches and data linking. Individuals are thus exposed to architectural problems that introduce the possibility of additional information-based harms, not necessarily a single, direct and harmful outcome. In this chapter, I have outlined the major conceptualizations of privacy and argued that these conceptions are largely incompatible with the need to seek simultaneous information sharing and protection in the health domain. I presented an approach to reconceptualizing privacy through a sociotechnical lens and provided evidence for the value of privacy, validating efforts to pursue protective measures while accommodating the need for informational continuity of care. In the following chapter, I will discuss how I have applied this reconceptualization on a specific case, supporting the importance of contextuality in the realm of privacy.

Chapter 4. Methods

4.1. Introduction

The following chapter will introduce the methods employed in this research. I will begin by contextualizing the research by describing the case I use to apply and further explore the concepts introduced thus far. I will then present the research questions that guided the project, followed by an outline of the methods of data collection and analysis, including the ontological and epistemological orientations that informed these decisions.

4.2. Case

This research situates the ethical dilemmas of information sharing and protection in health in the context of the development and implementation of a novel system to enable the documentation and communication of adverse drug events (ADEs) across health care settings in BC. This system, titled *ActionADE*, is part of a broader research program that studies the incidence, preventability, and documentation of ADEs, which are the harmful and unintended consequences of medication use and a leading cause of emergency department (ED) visits and hospital admissions in Canada (Budnitz, Lovegrove, Shehab, & Richards, 2011; Lazarou, Pomeranz, & Corey, 1998; Nebeker, Barach, & Samore, 2004; Zed, et al., 2008). Studies have found that between 30% and 70% of ADEs are preventable, many of which are repeat events (Classen, Pestotnik, Evans, Lloyd, & Burke, 1997; Gurwitz, et al., 2003; Zed, et al., 2008). There is a strong need for an effective communication system that would increase informational continuity of care about ADEs, while also reducing the risk of re-exposure to harmful medications.

Presently, there are a number of systems that are available for care providers and patients to report ADEs to government entities (e.g., MedEffect Canada, developed by Health Canada), independent organizations (e.g., the Council for International Organizations of Medical Sciences, via CIOMS Form I), or directly to pharmaceutical manufacturers. Despite existing mechanisms for reporting, research has illustrated that, on average, fewer than 5% of events are reported (Hohl, Lexchin, & Balka, 2015). Literature relating to this phenomenon of underreporting has identified a number of barriers to reporting ADEs, including lack of time, diagnostic uncertainty, lack of

awareness of how to report, and physician's attitudes (Hazell & Shakir, 2006; Vallano & et al., 2005). Generally, these perspectives focus on the human actors involved. Our project has been founded upon the notion that it is not solely the human factors that come to bear on reporting. We posit that a significant barrier to reporting is the incompatibility of the tools used to mediate the reporting and the sociotechnical processes within which they are situated (Hohl, Lexchin, & Balka, 2015). *ActionADE* is intended to fill the void of existing reporting mechanisms by focusing instead on supporting patient-specific outcomes, and clinician-oriented design, in order to foster positive health outcomes and facilitate communication between care providers and across care settings.

ActionADE is being developed by an interdisciplinary team of clinician scientists, social scientists, pharmacists, epidemiologists, and clinical pharmacologists. The project has been undertaken through a participatory design methodology, informed by sociotechnical principles. Several publications have been produced that discuss the methodological approach and findings to date, including a systematic review of existing ADE reporting systems worldwide, a series of iterative workshops among clinician end-users to establish data fields and form structure, and pilot testing the structure in a paper-based format in acute care settings (Chruscicki, et al., 2016; Bailey, et al., 2016; Peddie, et al., 2016). Through *ActionADE*, it is our intention that patient-specific ADE information will be documented and communicated across a patient's circle of care effectively and efficiently. This will then reduce a patient's risk of re-exposure to harmful medication and hopefully lower the rate at which individuals suffer repeat ADEs, and as a result, improve patient outcomes. Privacy concerns that emerge out of the introduction of novel flows of health information are applicable in this context.

ActionADE is being developed in BC and therefore will be situated within the federalist Canadian health care system. The Canada Health Act, a piece of federal legislation, identifies the guiding principles for health care that are then enacted provincially and territorially (Department of Finance Canada, 2011). Health care is publicly funded and delivered both privately (e.g., in doctors' offices) and publicly (e.g., at hospitals). Under this model, most services are free at the point of care. The funding is provided through a mix of federal and provincial funding. Federally, the government of Canada provides the provinces with funding through the Canada Health Transfer (CHT) (Department of Finance Canada, 2011). Payments are made on an equal per capita

basis through cash transfers (Department of Finance Canada, 2011). In the 2015/16 fiscal year, BC received $4.5 billion in funding through the CHT (BC Auditor General, 2017). In addition to the CHT, the province agreed to receive an additional $1.4 billion over the next ten years to specifically support home care and mental health services (BC Auditor General, 2017; Health Canada, 2017). Provincial funding for the Ministry of Health comes from such sources as taxes and fees. In the 2015/16 fiscal year, 37% of all provincial funding allocations from all sources (including the CHT) went to the Ministry of Health. The Ministry then redistributes this funding to the health authorities and other regional services (which are responsible for the delivering and planning of care in their respective geographic areas), the Medical Services Plan (MSP) to fund physicians (which is the public insurance coverage in BC), and PharmaCare (which provides coverage for prescription drugs) (BC Auditor General, 2017).

This thesis has been dedicated to an exploration of privacy concerns from a patient-oriented perspective, as well as the broader sociopolitical and technical elements that will come to bear on the implementation of *ActionADE*. Below, the research questions that have guided my inquiry will be presented, as well as the methods and design that enabled an exploration of these questions.

4.3. Choice of Methods and Research Design

I posed a series of research questions aimed at understanding the sociotechnical and political landscape into which *ActionADE* will be introduced, particularly in relation to privacy issues:

> RQ1: What is the current policy environment surrounding health data privacy in BC, at both institutional and governmental levels?
>
> RQ2: What are patient perceptions and attitudes about information sharing in relation to information privacy?
>
> RQ3: How can these insights inform the development of *ActionADE*?

To address Research Question 1, I referred to existing literature and materials. This consisted of an analysis of legislative frameworks and other relevant policy documents at the institutional, provincial, and federal level. I relied on additional resources available from the OIPCBC and the Office of the Privacy Commissioner of Canada.

In response to Research Question 2, I undertook an independent analysis of a series of focus groups that were conducted among patients as part of the *ActionADE* research program. Focus groups were deliberately selected as the research method due to the advantages they afford. Early uses were largely employed for research in marketing and advertising, based on the research conducted by Paul Lazarsfeld and Robert Merton in the 1940s (Bernard, 1995). By the 1980s, focus groups became widely used in research, both alone and in conjunction with other quantitative methods (Bernard, 1995). Led by a moderator, a focus group is a group-based discussion with open dialogue on a particular topic. Focus groups permit the collection of a diversity of views simultaneously and enable the exploration of individuals' rationales underpinning their perspectives. The capacity to ask the key question 'why' enables an in-depth discussion on a given topic, particularly when compared to closed-ended questionnaires or surveys (Bernard, 1995).

Unlike one-on-one interviews, focus groups are uniquely positioned to foster rich debate among participants, illuminating apparent contradictions and, in some cases, triggering changes in opinion (Barbour, 2008). A successfully moderated focus group encourages an environment of trust and mutual respect among participants, thereby eliciting lively conversation and, in some cases, a discussion on topics that might otherwise be considered sensitive (Bernard, 1995). Furthermore, focus groups shift emphasis away from the researcher's perspective and onto that of the participants, generating open dialogue and new ideas (Barbour, 2008). As a consequence, focus groups can produce a rich data set with divergent viewpoints, in-depth perspectives, and dynamic discussion. In the context of this research, these are particular advantages as issues related to privacy of health data are often hotly debated and may be considered sensitive to some.

The rationale for conducting research among a patient and family and friend caregiver sample was threefold. Firstly, this methodology is a direct response to the status quo whereby the preferences and attitudes of patients about information sharing in care contexts are assumed throughout the design and implementation of health ICTs, particularly concerning their privacy. It is often the case that policymakers and system designers make the key decisions surrounding the type of information shared and not shared, and under which circumstances. Patients are thus constructed as implicated actors in this situation. Therefore, this methodology presents an opportunity for patients

to be drawn out of their implicated status to a more active position where they can contribute meaningfully to the development of an ICT that will mediate the flow of their information.

Secondly, this project is situated within the broader movement toward patient engagement and involvement in health research and interventions. It was the intention of this project that involving patients will ensure that the system serves the needs of its users, while also conforming to the expectations and preferences of individuals that have a stake in it. Literature on patient engagement has suggested that this type of involvement is advantageous for all parties, as patients bring fresh perspectives and lived experiences to the benefit of researchers, resulting in research and systems that serve the needs and desires of those individuals (Nass, Levine, & Yancy). In this instance, patients provided novel insights and perspectives that will be discussed in the following sections, while we intended to impart upon them knowledge related to the status quo of information sharing, both throughout the discussion and in a debriefing document that was provided following the sessions (see Appendix A).

Lastly, this method represents a practical application of theoretical constructs that demand contextual and situational analysis of novel ICTs and the resultant flow of information and concerns related to privacy that were discussed above. Studies on privacy that account for patient perspectives are often undertaken through survey methodologies, which do not lend themselves to the same degree of depth of analysis afforded in qualitative research (Nissenbaum, 2010). These surveys are insufficient because the question format does not enable the researcher to establish links between responses and the contextual norms that affect perceptions and behaviours (Nissenbaum, 2010). Through this approach, conclusions are drawn from and applied to real life circumstances to produce more robust research methodologies and improved system outcomes.

We extended the sample to include friend and family caregivers in this context as well, because it is often the case that patients, especially older patients, are not independently responsible for the maintenance of their health. Informal caregivers are often tasked with navigating the health system on behalf of patients, providing information to and receiving information about the patients to their different care

providers. Caregivers, therefore, experience the same implicatedness, barriers, and engagement as the individuals that they care for.

To complement the data collected through the focus groups, it is often recommended that findings are contextualized against existing survey data, in order to increase the robustness of both data sources (Bernard, 1995). As such, the findings from these focus groups were compared to existing survey data conducted among Canadians in relation to the privacy of health data. This will provide a greater degree of contextuality and situatedness that has been advocated for in previous chapters. There have been numerous survey undertakings that concern data privacy in health in Canada, but this research will focus on two specific cases.[1] The survey data that will be discussed in relation to the focus group data has been drawn from Phoenix Strategic Perspectives Inc.'s (2013) report titled *Survey of Canadians on Privacy-Related Issues* and Ipsos-Reid's (2012) report titled *What Canadians Think: Electronic Health Information and Privacy Survey 2012*. The Phoenix Strategic Perspectives survey was completed on behalf of the Office of the Privacy Commissioner of Canada to explore individuals' awareness, understanding, and perception of privacy. A telephone survey was completed among 1,513 Canadians aged 16 and above. The results from this survey were collected in 2012 and are considered accurate plus or minus 2.5% with a 95% confidence interval. The Ipsos-Reid survey was completed on behalf of Canada Health Infoway. The survey, conducted in 2012, was the second wave of a survey completed in 2007 by EKOS Research Associates, co-sponsored by Canada Health Infoway, Health Canada, and the Office of the Privacy Commissioner of Canada. The second wave of the survey was conducted among 2,509 Canadians aged 16 and older. The survey was administered online (n=1,209) and by telephone (n=1,300). The results from this survey are considered statistically accurate plus or minus 2% with a 95%

[1] This decision relates back to Nissenbaum's (2010) critique of public opinion surveys being vague and analytically limited. For example, Angus Reid has completed two recent surveys that were presented at the national Data Effect Conference in 2012 and 2013, both of which concern health information privacy, but both are of limited value. The 2012 publication featured four questions about the use of 'depersonalized data' for research, but they do not differentiate support for different kinds of research (e.g., university-based vs. privately sponsored) until the final question. This may have biased responses. The 2013 poll is similarly confusing, by first asking about the use of 'personal health care data' and then 'public data' – neither of which are defined, yet were asked sequentially, which may have also been confusing. Additionally, neither survey offered the same scope of questions that were explored in the two that were selected for this research. (See Angus Reid Public Opinion, 2012 and Angus Reid Public Opinion, 2013)

confidence interval. No future waves of this survey were completed on behalf of Canada Health Infoway.

4.3.1. Discussion Guide Design

A discussion guide was developed to direct the focus groups and highlight key thematic elements drawn from the literature and from existing surveys about the privacy of health data (Appendix B). Broadly, the key thematic elements of the discussion guide addressed preferences and perceptions related to information sharing, experiences with adverse drug events, and attitudes about data privacy. The discussion guide was not intended to be a firm script from which each group would follow. Rather, this guide served as a template with room for natural conversational flow and digressions where appropriate, while ensuring that the thematic elements were addressed. As a result, participants were afforded the opportunity to ask questions, engage in open dialogue, and identify and elaborate on new concepts that had not yet been considered. The guide was developed collaboratively among members of the *ActionADE* project team. The distinct disciplinary orientations of each team member offered a variety of unique perspectives on the content, thereby enhancing the robustness of the guide.

4.3.2. Recruitment

The study population of patients and caregivers encompasses a large diversity of individuals with highly unique lived experience and level of interaction with the health care system. This emphasizes the need for inclusivity in the recruitment of focus group participants. Accordingly, research ethics board approval was secured to recruit through multiple avenues. Recruitment strategies to reach an older patient cohort began with personal connections of the principal investigators. To reach individuals that interact with the health system, posters were posted in the ED and in the lobby of the Research Pavilion at Vancouver General Hospital (VGH), and active recruitment was undertaken in the ED of VGH by a research assistant. To reach a broader population, advertisements were also posted on the free classifieds websites Kijiji and Craigslist, in addition to a post on the *ActionADE* website (actionade.org).

Of these methods, the most successful means of recruitment was active recruitment in the ED, wherein 20 individuals agreed to participate. Although this was the

most successful means of recruitment, it was also the most labour intensive. In contrast, online advertisements on Kijiji and Craigslist solicited the interest of 13 individuals and required very little effort on behalf of the research team. This method did see a slightly higher rate of attrition, however, as only 38% of those who agreed to participate actually did (compared with 45% of those recruited in the ED). Regardless, in light of the time and labour investment of both methods, the online advertisements may be interpreted as more successful. The least successful means of recruitment were the posters posted in the ED and lobby of the Research Pavilion at VGH, which collectively solicited the interest of two individuals. Table 1, below, illustrates the number of participants that contacted the research team as a result of each recruitment method, and, of those, the number who were able to join one of the scheduled focus groups.

Table 1. Recruitment Strategies

Recruitment Method	# Agreed to Participate	# Attended
Personal connections	5	5
Posters in ED and Research Pavilion Lobby	2	1
Active recruitment in ED	20	9
Online advertisements	13	5

While participation was compensated with an honorarium, this fact was not explicitly advertised in the recruiting efforts. This was undertaken with the intention of ensuring that those who volunteered for the study were genuinely interested in the subject matter, rather than simply the honorarium. On the other hand, however, this may have had a negative impact on the overall number of responses received.

4.3.3. Inclusion / Exclusion Criteria

Although recruitment in the ED placed a greater emphasis on those who were at risk of or who had already experienced an ADE, this was not the exclusive criteria for participation. In keeping with the literature on patient engagement, we acknowledge the idiosyncratic nature of the patient experience. Therefore, the inclusion and exclusion criteria for this undertaking remained quite broad. Formally, the inclusion criteria were limited to those residing in the Lower Mainland and Whistler, BC. This strategy was twofold: firstly, logistically, maintaining a geographic boundary would facilitate the planning of the groups; secondly, this would also ensure that the participants lived within the contextual reality of the *ActionADE* system. Lastly, although the recruitment strategy

strove for inclusivity, it is acknowledged that achieving representativeness in this endeavour is not possible, given both the recruiting methods and the diversity of patient and caregiver populations, nor was it a goal of the project.

4.3.4. Data Collection

Each focus group was 120 minutes in duration. Three focus groups were completed in November and December, 2016, with 5 to 8 participants per group. There were 20 participants in total. Participants were provided with a meal during the group and received a $30 gift card to London Drugs (a chain of retail stores that sell a range of everyday products, from milk to lawn care products, electronics and small appliances, as well as the traditional contents of a drug store) at the conclusion of the session. Focus groups were moderated by Dr. Ellen Balka and attended by other team members to observe and take notes. Participants completed written consent forms at the beginning of the session. The sessions were audio recorded and then transcribed with all participant identifiers removed. Followed the transcription, audio records were destroyed, eliminating the possibility for re-identification. Written notes supplemented the audio transcription to capture non-verbal cues, such as gestures, which increased the robustness of the data. The transcriptions ultimately reflected a range of interactions beyond simply audio material, including pauses, interruptions, silences, laughter, and gesturing, where possible. The transcripts were stored on the secure UBC network, which only the *ActionADE* team members had access to.

At the conclusion of each focus group session, participants were asked to complete a follow up survey that included some demographic information. Eighteen out of 20 participants completed the survey, therefore the following description is accurate minus two individuals who opted not to complete the survey. Twelve participants were female and six were male. The youngest participant was 21 and the oldest was 77, with the median participant age at 59 years old. Level of education of participants was generally quite high: ten had completed college or university; four had completed some college or university; two had completed some graduate school; two had completed high school; one had completed some high school; one had completed a Master's degree; one had completed a doctoral degree; and one participant did not respond to the question. Thirteen participants had either experienced an ADE (3), knew someone that had experienced an ADE (6), or both (4); 4 participants reported that they had not

experienced an ADE nor had anyone they had known; one person was not sure. These characteristics indicate that our participants likely had a high stake in the *ActionADE* system due to the relatively older median age and experiences with ADEs.

4.3.5. Coding and Data Analysis

Findings from the focus groups were coded and analyzed qualitatively using NVivo 11 Software. A provisional coding frame was established *a priori* to reflect the thematic structure and questions that were included in the discussion guide. Through an iterative process, the provisional coding frame was revised, in keeping with the process of open coding in traditional grounded theory (Glaser & Strauss, 1967). Open coding involves the reading and re-reading of transcripts to establish new codes and sub-codes, collapse and expand codes, and delete codes (Barbour, 2008). See Appendix C for the node structure. Following the preliminary coding, analysis proceeded according to Adele Clarke's (2005) situational analysis.

The Theoretical Origins of Situational Analysis

Situational analysis is a theory/methods package. The epistemological and ontological roots of situational analysis rest largely in grounded theory and the social worlds and arenas framework. Grounded theory, developed by Anselm Strauss and Barney Glaser (1967), presents an approach to the study of basic social processes through qualitative methods. Grounded theory inductively derives theory from data. This is in direct contrast to the previously pervasive positivist research methods that employ quantitative data, analyzed deductively to validate existing theories (Clarke, 2005). Grounded theory emphasizes interactionist constructionism and action-centered negotiations and processes, with a particular focus on the complexities and realities of subjectivity in research (Clarke, 2005). Researchers are advised to begin coding as soon as data collection begins, typically using ethnographic or interview data (Clarke, 2005). This form of open coding enhances critical analysis and highlights the differences and silences in data. Coding is to be completed iteratively throughout the research process, which then presents the emergence of relevant theoretical constructs. This form of data collection and analysis that informs emergent theories is referred to as 'theoretical sampling' (Clarke, 2005).

Clarke (2005) acknowledges the value of these tools in qualitative research, but argues that grounded theory requires modification to reflect the postmodern context. In particular, Clarke notes that some of the principles of traditional grounded theory err too heavily on empiricism and positivism. For example, the importance of reflexivity on behalf of the researcher is wholly absent from the tenets of grounded theory. In the absence of reflexivity, the researcher fails to acknowledge their own biases, goals, and perspectives that impede upon the research process (Clarke, 2005). A lack of reflexivity leads to assumptions that skew the data. Another problematic element of traditional grounded theory is the tendency toward oversimplification. This, too, introduces the possibility of misrepresenting the data.

Through the adoption of many of the key analytical principles of grounded theory, supplemented with novel principles that are more relevant to the postmodern context, situational analysis forms a 'conceptual infrastructure' that focuses on situatedness, heterogeneity, and instability (Clarke, 2005). According to Clarke (2005), the methodological implications of the turn toward postmodernism include an acknowledgement of this complex reality, as well as a consideration of the contextual positionality and relationality. This includes transparent and explicit reflexive elements, thereby rejecting the veil of objectivity through continual memo-ing and an acknowledgement of one's own role in the research process. Furthermore, situational analysis avoids oversimplification through an explicit emphasis on the messiness and complexity of the real world. Situational analysis also expands the scope of grounded theory by taking into account the narrative, visual, and historic discourses that come to bear on the situation. As such, the researcher may then begin to develop concepts that reject normative constructions of the world, presenting instead a multidimensional, "thick analysis" (Clarke, 2005, p. 29).

Overview of Situational Analysis

Situational Maps

The analytic and reflexive exercise of situational analysis is undertaken through simultaneous coding, mapping, and memo-ing, using the situation itself as the unit of analysis. Central to this approach is the use of three cartographic exercises that enable a dynamic and responsive research process, allowing space for new insights and reflexive reflections. The first mapping process is referred to as situational mapping,

which involves an articulation of the different components of the situation, and subsequent mapping of the relations between those components (Clarke, 2005). Working with at least partially coded data, this process begins by developing a messy version of the map that identifies all the human and non-human actors, discourses, and symbolic and material elements in the situation. This process is undertaken iteratively until the researcher achieves a point of saturation with the data, although it is unlikely that every aspect of any given situation could be addressed due to the inherent messiness and complexity of the situation. Upon reaching the point of saturation, the different actors, discourses, and elements are mapped into an ordered version based on a set of categories drawn from Strauss and identified by Clarke (2005), as well as any additional categories that might be considered important or valuable to the situation. Following this mapping, a relational analysis is undertaken to identify the nature of the relationships in the situation (Clarke, 2005). Throughout the duration of these exercises, the researcher must be memo-ing, a key component of the reflexivity identified above. Overall, situational mapping enables the researcher to understand the relevant elements and aspects in a situation and the relations between them. For this research undertaking, relational analysis has been facilitated by situational mapping for a number of key actors and themes. The intention of the relational analysis is to unpack the complex sociotechnical reality, attempting to understand the situation as a whole through the relations between these elements. The key components of the current situation that served as the basis for relational analysis are: privacy policy, secondary uses of health data, information-based harms, and informational continuity of care.

Social Worlds and Arenas Maps

The second cartographic approach is the social worlds and arenas map. Social worlds and arenas maps, drawn largely out of Strauss' work on social worlds, arenas, and negotiations, consists of identifying the collective actors, important non-human actants, and their arenas of commitment. The goal of this exercise is to visualize the relationships that are either the subject of, or shape the subject of, the research (Clarke, Friese, & Washburn, 2015). Focusing on collectivities, this mapping is intended to situate the research more broadly by focusing on the meso level. Social worlds are groups of individuals that converge on the basis of a shared area of concern or commitment (Clarke, Friese, & Washburn, 2015). Of note, this includes an examination of reluctant and absent participants, which distinguishes it from other organizational theories. The

arena represents the site of convergence of these different social worlds. In these maps, dotted lines are used to illustrate the porousness of boundaries and the multiplicity of overlapping social worlds. Using the conceptual toolbox that Clarke provides (2005, see p. 112), as well as continual memo-ing, the researcher is tasked with understanding these fluidities, specifying differences and variations within and between worlds, and understanding sites of conflict. Following the initial mapping, the social worlds and arenas map becomes the base from which further interrogation proceeds. Clarke (2005) notes that the researcher may choose to continue deeper into the analysis of social worlds and arenas, or they may proceed to the third cartographic exercise, positional mapping. For the purposes of this thesis, positional mapping was taken as the next step.

Positional Maps

Positional mapping identifies discursive components in the data, particularly in terms of the positions taken or not taken. Positions are independent of individuals or collectives, and focus on marginalities and heterogeneities. The independence of positions relative to actors is an acknowledgement of the fluidity of positions, which may change in different situations and contexts. It also eliminates the tendency to reduce discourse into binaries and arranges positions dimensionally across axes that are defined in terms of what is more or less. Another key element is to indicate the missing positions in the data. Positional mapping in this context was undertaken for only one discursive aspect of the research, which was to understand the discursive construction of the need to protect privacy relative to the need to share information.

4.4. Conclusion

In this chapter, I have introduced the methods employed in this research undertaking. I described the *ActionADE* research project as the site of the research. I identified the research questions that guided the design and then discussed the methods used to respond to those questions. I discussed the details related to the data collection through focus groups, as well as the analytical strategy used. In doing so, I provided an overview of the theoretical underpinnings that led to the development of situational analysis and discussed its practical application.

Chapter 5. Situating Privacy and Information Sharing in *ActionADE*

5.1. Introduction

Using evidence from the focus groups, supplemented by relevant policy documents, public opinion surveys, and other literature, the following section will provide a detailed analysis of information sharing and privacy concerns in the context of the design and implementation of *ActionADE*. First, I will situate *ActionADE* within the privacy policy landscape into which it will be introduced. This contextualization will be enabled by Clarke's (2005) social worlds and arenas map. It will provide an understanding of the legislative regimes and key collective actors that will come to bear on the system from a policy perspective. Second, I will present an analysis of the focus group findings, exploring patient preferences and perceptions about medication information sharing and the privacy policy landscape. Drawing from the relational analysis completed during the situational mapping phase, these findings will be situated within the broader context of *ActionADE's* implementation. This section will also address the overarching question of how to balance information sharing and information protection, analyzed and visualized through a positional map, permitting an exploration of the different discursive positions that were both taken and not taken in the data. Lastly, drawing from the preceding sections, I will discuss the ways in which the design and implementation of *ActionADE* can be optimized to manage patient expectations and legislative demands through a series of recommendations.

5.2. Situating *ActionADE* in the Policy Landscape

An important first step in approaching privacy issues related to the information flows that will be mediated by *ActionADE* is contextualizing these flows within the formal privacy conditions that will come to bear on the system. I have used Clarke's (2005) social worlds and arenas mapping to facilitate this portion of the analysis, with the intention of visualizing the social relations that shape the privacy policy landscape and the relevant artefacts that emerge out of these relations. Within this conceptualization, a social world is defined as a group of actors that converge under an umbrella of shared interest or concern (Clarke, 2005). Each group has a particular stake in the discursive

construction of the privacy policy landscape in which *ActionADE* will exist. These social worlds and the corresponding research topic exist within a broader area of concern, referred to as the social arena. The social arena represents the site of convergence of several social worlds over time. This mapping enables the identification and understanding of the different hierarchies that exist within this situation, delineating central and marginal actors involved, as well as the discourses and technologies that are employed to meet their ends. This clarifies the way in which different conceptions of the research subject emerge out of these social worlds.

In the map (Figure 1), each circle represents a unique social world, grouped together within the broader social arena under which they are converging. The dotted lines represent the porousness of the boundaries of these worlds, in recognition that social worlds are not mutually exclusive and individuals may cross the boundary of one world into another at any given time. Each element of Figure 1 will be elaborated on below.

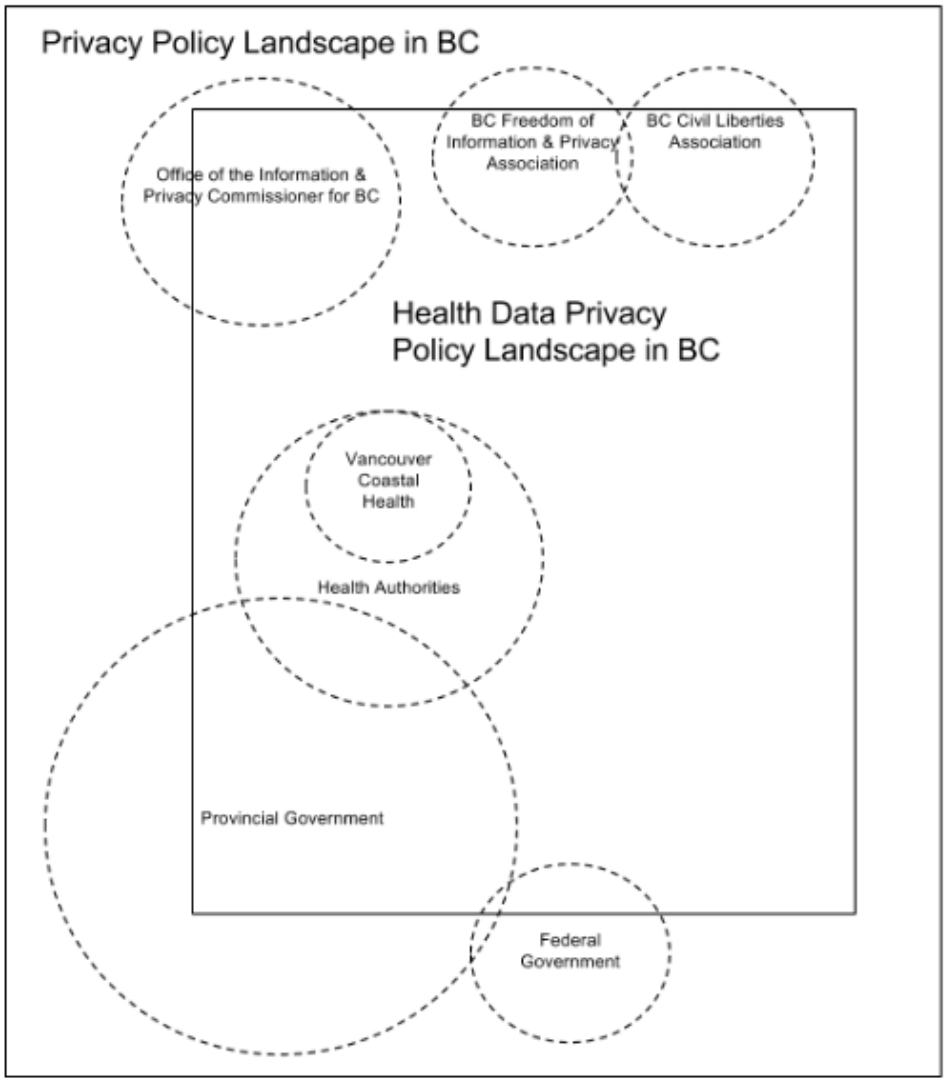

Figure 1: Social Worlds & Arenas Map of the Policy Landscape

5.2.1. The Provincial Government

In this map, I suggest that the provincial government is the central actor by the relative size of its circle. Legislation established by the provincial government governs much of the flow of information and data privacy provincially. In BC, there are two pieces of legislation that have been produced by the provincial government and are central to data privacy, representing key political elements in the situation: the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Information Protection Act (PIPA). FIPPA pertains to the collection, use, and dissemination of information by public entities, consisting of health authorities, hospitals, and other publicly provisioned health services. It requires that these entities provide and enforce

security measures to prevent unauthorized collection, use, access, disclosure, and disposal of personal information. Upon initial data collection, FIPPA requires that public entities provide information related to the purpose of the data collection and contact information to whom individuals may direct further inquiries related to the data collection and use (OIPCBC, 2015a). This may be understood as a principle of notification. The disclosure of the data beyond initial collection requires written consent, although there are exceptions. For example, for public health and safety purposes, consent is not required. Under Section 35, FIPPA delineates conditions under which personal information may be disclosed for research purposes (i.e., a secondary use of data) as well.

Whereas FIPPA applies to public sector entities, PIPA concerns the collection, use, and dissemination of information by private entities. Therefore, PIPA applies to such care providers as doctors' offices, private imaging clinics, community pharmacies, and so on. Consent is a key component of information collection, use, and sharing under PIPA. Consent is granted when an individual provides their personal information voluntarily with an understanding of the purpose of the collection. Different types of consent are permissible under PIPA, depending upon the circumstance. Express consent is akin to verbal or written consent, wherein an individual explicitly agrees to the conditions under which their information is to be collected, used, and disclosed (OIPCBC, 2015b). Deemed consent refers to the voluntary information sharing that occurs in circumstances in which the purpose is obvious and reasonable (OIPCBC, 2015b). Lastly, consent by not declining consent echoes the principle of notification employed in FIPPA while also affording the individual an opportunity to opt out (OIPCBC, 2015b). Any secondary uses of data beyond that for which the information was initially collected requires consent, although exceptions apply in this context as well, such as in compliance with legal demands.

Of note, neither FIPPA nor PIPA pertain exclusively to health information, a fact represented by the provincial government's positioning in the broader arena of privacy policy as well as the arena specific to health information in Figure 1. This may be contrasted to the American context, whereby privacy legislation is sectoral, meaning that there are distinct pieces of privacy legislation that apply to different arenas. In the US health domain, health data are governed by the Health Insurance Portability and Protection Act (HIPPA) Privacy Rule (Health and Human Services, 2014). In the

Canadian context, the umbrella legislation presents a health privacy policy arena that exists within the broader arena of data privacy. The broader arena is therefore home to a multitude of other smaller arenas and social worlds, in such sectors as national security, education, and so forth. These other collective actors have not been illustrated in Figure 1 in order to streamline the scope of this undertaking.

The lack of definitive sectoral legislation concerning the privacy of health data demands additional political elements. Beyond FIPPA and PIPA, other legal provisions related to personal health information that have been advanced by the provincial government are scattered throughout other pieces of legislation. These include the E-Health Act, the Pharmaceutical Services Act, the Ministry of Health Act, and the Public Health Act, which contain various affordances related to information collection, use, and protection by the Ministry of Health and beyond. As one might expect, this structure leads to a highly fragmented and difficult to understand legislative environment.

Situating *ActionADE* within this complex and ambiguous legislative framework will be contingent upon its implementation, particularly in terms of how the data are collected and stored. It is likely that the information in *ActionADE* will be collected by public bodies, such as hospitals or health authorities. Therefore, the provisions in FIPPA would apply, even if the information is being accessed and used contractually by private entities, such as community pharmacies. In the event that *ActionADE* is integrated into existing infrastructure, this may vary. For example, BC's PharmaNet is an electronic system used primarily for billing in community pharmacy settings, and also accessed by some public (e.g., hospitals) and private (e.g., family physicians) entities for medication management and care purposes. PharmaNet and the data contained within it are governed by the Pharmaceutical Services Act, which is separate from but compliant with FIPPA. If *ActionADE* is integrated into PharmaNet, the governance of data stored in PharmaNet would fall primarily within the scope of the Pharmaceutical Services Act.

5.2.2. The Health Authorities

In BC, six health authorities are responsible for the delivery and planning of most of the publicly funded health services in the province (BC Auditor General, 2017). The six health authorities consist of five regional authorities with defined geographic zones, as well as the Provincial Health Services Authority, which provides province-wide,

specialized health services in collaboration with the Ministry of Health and the other health authorities (BC Auditor General, 2017). Patients may seek care in different health authorities at any given point in time (in addition to from private sector care providers), pointing to the need for data sharing both within and across jurisdictions, in support of informational continuity of care. The efficacy of this information sharing, however, is rarely as successful as it should be, a finding that will be explored in section 5.3.

The initial implementation *of ActionADE* will be within Vancouver Coastal Health (VCH), a public health authority that is governed by FIPPA. Health authorities, including VCH, are responsible for the operationalization of FIPPA through institutional policies and procedures. The VCH Information and Confidentiality Policy delineates proper procedures related to information collection, use, disclosure, consent, security safeguards, and data retention at all VCH sites. VCH complies with FIPPA's principle of notification through VCH Client Notification Sign, which is posted at all registration, intake, and admission sites. This sign includes the following statement with regard to data collection: "Your information may be entered into our electronic health information systems to assist authorized persons in quickly accessing pertinent information wherever you may be receiving care or services" (VCH, 2012). As a result, information collected and shared via *ActionADE* will not demand any additional consent requirements at the point of care. This is in the interest of care providers and is intended to facilitate informational continuity in the clinical setting. For patients, this may be a site of tension between information sharing and information protection, as they would likely have a stake in care providers' efficient and easy access to patient information, but there is a question of whether the Client Notification Sign is sufficient to inform patients of their informational rights.

5.2.3. The Federal Government

The federal government is responsible for policy setting at the national level. There are two key pieces of legislation related to privacy and information sharing at the federal level. The Privacy Act governs the way in which personal information is collected, used, and stored by the federal government. At present, the Privacy Act will have no jurisdiction over personal information collected by *ActionADE* because the data will be contained within the province of BC. This may change, however, due to forthcoming regulations related to the mandatory reporting of adverse drug reactions (ADRs), a

subset of ADEs. In 2014, the federal government introduced a series of amendments to the Food and Drugs Act, titled Vanessa's Law. Section 21.8 of Vanessa's Law mandates this reporting. The details surrounding this portion of the legislation have yet to come into effect at the time of writing, but upon introduction it may require that health authorities collect and report *ActionADE* data to the federal government.

The second political element at the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA), concerns the collection, use, and disclosure of information in the private sector. PIPEDA only applies provincially in the event that substantially similar provincial legislation does not exist. In BC, PIPA has been deemed to be substantially similar legislation, therefore PIPEDA does not apply. Due to the limited applicability of the federal legislation in the context of *ActionADE*, it is presented as a marginal actor in Figure 1.

5.2.4. The Office of the Information & Privacy Commissioner for BC

The OIPCBC provides independent oversight of privacy-related issues in the province. The OIPCBC monitors compliance with both FIPPA and PIPA, conducts independent research on relevant privacy issues, and provides public education on issues related to data privacy. The OIPCBC has criticized the current data privacy legislation, particularly as it relates to medical data. In 2014, an OIPCBC report argued for reform of the current legislation to meet the unique needs and demands of data sharing and protection in health. The recommendations included enhancing the transparency of data flows and permitting secondary uses exclusively for health-related activities. The role of the OIPCBC is tangential to *ActionADE*, in that the OIPCBC would only be involved in the event that a complaint is launched and the system is involved.

5.2.5. Patient Advocacy Groups and Patients

Of note, patients are absent from this map, illustrating their role as implicated actors in the situation. Patients and patient interests are instead represented by various advocacy groups. In this map, I have included the BC Freedom of Information and Privacy Association (FIPA) and the BC Civil Liberties Association (BCCLA). FIPA is a nonpartisan, non-profit entity that was established in 1991. Its mandate is to champion information and privacy rights through citizen empowerment, public education, public

assistance, research, and law reform (FIPA, 2017). The BCCLA, established in 1962, operates more broadly than FIPA. Its mandate is to support individual rights and freedoms across a spectrum of issues beyond information privacy (BC Civil Liberties Association, N.D.). Although their mandate is broad, they have demonstrated their stake in representing individual privacy interests, as evidenced by frequent reports, presentations, and commentaries about issues related to online surveillance and data privacy in the digital era (BC Civil Liberties Association, N.D.).

Despite representation from FIPA and the BCCLA, patient preferences and attitudes related to the sharing of their information are largely assumed, and therefore may or may not be reflected in policy. Recently, for example, the BC government began to introduce a combined Driver's Licence and Services Card to replace the previously independent driver's licences and CareCards (the provincial health care card). In advance of the project roll out, FIPA and the BCCLA conveyed concerns regarding individual privacy in the context of these cards, particularly as the government had intended to mandate the combination of health data and other information as of 2018 (BCCLA, 2013; FIPA, 2013a). The BCCLA and FIPA jointly sent a letter to the Minister of Technology, Innovation and Citizens' Services concerning the credibility of the public consultation and created a corresponding campaign, citing that those consulted were being denied the ability to recommend stopping the program, and that the consultative method whereby citizens are given pre-determined scenarios electronically limits public participation (FIPA, 2013b). At the conclusion of the consultation, the citizen panel recommended against making the combined card mandatory as of 2018, although the program still came into effect with the option to either combine driver's licence and health care or keep them separate (FIPA, 2013a; FIPA, 2013b; FIPA, 2014). Problematically, current online resources concerning the combined Driver's Licence and Services Card do not explicitly advertise the option to keep them separate, which may have an effect on the extent to which individuals are aware that they do not have to combine their cards (for example, see Government of British Columbia, N.D).

Indeed, it has been noted that policy development is often established based on the experiences of the policymakers, not based on those to whom the policy relates and is intended to benefit (Clarke, 2005). Through the focus groups, patients were given the opportunity to express perspectives in an arena in which they are often relegated to the margins. Therefore, in this research undertaking, I have challenged the normative

decision-making structure related to policy design that is presented in the social worlds and arenas map above (Figure 1). Patient perceptions on issues related to information sharing and information privacy within the context of *ActionADE* will be discussed below.

5.3. Patient Perceptions toward Information Sharing and Privacy in the Context of *ActionADE*

The focus groups followed a semi-structured discussion guide to address a number of key thematic elements that were identified *a priori* based on the literature and existing studies. The following section will present the key findings from the focus group sessions. The relational analysis that was undertaken through the situational mapping phase enabled the contextualization of focus group findings within the broader sociotechnical and political environments (see Appendix D). In response to the status quo whereby patients are marginalized and implicated in policy settings, I begin by discussing participants' preferences and perceptions toward the current policy landscape. I then present an analysis of the key thematic elements that both guided and emerged organically out of the focus group sessions. The major themes that will be discussed are informational continuity of care, the secondary uses of health data and consent, and privacy and security related to health data. Throughout, the findings will be contextualized in the broader Canadian context based on public opinion survey results.

5.3.1. Patient Perspectives toward Privacy Policy

Participants were asked two streams of questions about the topic of privacy legislation. First, we sought to understand their awareness of and perceptions about the legislative regimes that come to bear on the flow of their information. These questions were intended to gauge the extent to which the participants were engaged with the policy landscape. Second, we sought to understand participant perceptions about the different central actors as policymakers. These questions sought to address the level of acceptance surrounding the central actors involved in policymaking.

Familiarity with Legislative Environment

The majority of participants reported awareness of the legislation that protects their confidential medical information, but few were able to name the legislation. Among those who elaborated, responses merely touched upon the legislative reality. One

participant alluded to FIPPA, referring to it as “Freedom of Information Act” (Participant 4), while another pointed to the policies published by the College of Physicians and Surgeons of BC (although they did acknowledge that it was not a law) (Participant 17). One participant made note of the BC physician privacy toolkit and mentioned policies related to PharmaNet, but was unable name the policy (Participant 8). The majority of participants were uncertain and did not offer a response, demonstrated by the following quote from Participant 8, who had taught courses in health information management prior to retirement: “Well I know generally and I used to know in detail, but no, I’m retired.” These findings are consistent with survey results, which indicate that many Canadians reported awareness of legislation that pertains to their privacy (52%), yet most (62%) were not sure of or did not know the name (Ipsos Reid, 2012). Another public opinion survey found that 63% of Canadians rated their knowledge of their legal privacy rights as low or neutral (Phoenix Strategic Perspectives Inc., 2013).

Following the initial question about awareness, we intended to ask participants about their perceptions toward the strength of the legislation in protecting privacy and the effect this legislation on the provision of care. Participants were given a handout with an overview of relevant legislation, but they were unable to fully digest the information and ask questions due to time constraints. As a result, when we posed the questions to the first group, participants were unable to provide an opinion. These questions were not asked in subsequent groups, although focus group participants were still given the handout that they were encouraged to take with them at the conclusion of the session (Appendix A).

Roles of Different Actors in Policy Setting

Despite generally low awareness of the policy landscape, participants were asked a series of questions about the central actors currently involved in privacy policy setting. First, we addressed perceptions about the provincial government as a privacy policymaker, followed by the federal government, and lastly the health authorities. Unprompted, participants provided other approaches to policy setting, which will be discussed as well.

The Provincial Government

The response was mixed when asked whether the provincial government should set policies related to privacy. On the one hand, it was noted that policy setting at the provincial level would centralize processes and therefore benefit individuals seeking care, particularly in the event that they sought care across multiple jurisdictions. Participants' comments demonstrated an awareness of temporal and spatial challenges associated with information sharing within the health care system, and supported a need for flexible systems and policies. Pointing to these advantages, Group A arrived at the consensus that the provincial government should be responsible for privacy policy setting. Others, however, were less enthusiastic. According to Participant 20: "I'm hesitant to see the provincial government make policy in anything quite honestly." Some expressed a sense of resignation in the tone in which they discussed policy setting at the provincial level, viewing it as necessary despite personal dissatisfaction with the government. Participant 15 stated: "We are bound by our nation state and provincial structure." These responses tend to align with the status quo whereby the provincial government is the central actor in setting privacy policy. A group of participants in Group A suggested that the status quo could be improved upon, however, by establishing a set timeline for the review of provincial policies to ensure relevance.

Others expressed comfort with the provincial government as a policymaker, but with caveats. Some stated that their support would be contingent upon which party was in power, which is an interesting position given the fact that, at the time of writing, the political future of BC is uncertain due to an upcoming vote of confidence for the recently elected BC Liberals. In light of this, I began questioning the extent to which perceptions toward the current ruling party came to bear on participant responses. For example, a number of individuals were critical toward the government as a policymaker due to bureaucratic inefficiencies and a poor track record. In particular, one participant questioned the government's capacity to develop effective privacy policy given its history of serious privacy breaches (Participant 15). As a result, perceptions toward the provincial government as a policymaker may shift following the vote of confidence if the current party does not earn a majority of votes.

The Federal Government

When asked about their comfort with the federal government as a privacy policymaker, participants had mixed opinions. Whereas one participant argued that the size of the country exceeds the federal capacity to regulate information sharing and privacy, another group concluded that federal policy setting could be advantageous because it could facilitate information sharing nationally and permit a broader view of national trends, which could then present opportunities for policy improvement and evaluation at the provincial level. Two participants in another group were more supportive of the potential role that Health Canada's could play in policy setting, noting that they may be better suited to establish a nation-wide policy that could then be implemented at the provincial level.[2]

Health Authorities

When asked about their comfort with the health authorities as a privacy policymaker, few participants expressed support. In Group A, the role of the health authorities elicited a debate about whether or not they would be more or less politically motivated than government actors:

> Participant 7: The nice thing about the health authority is that they're not as politically motivated as our politicians are.
>
> 8: Oh, disagree.
>
> 3: Disagree with that.
>
> 7: Well they shouldn't be.

Others stated that there would be too much duplication and too many competing priorities if health authorities were involved in policy setting. Several suggested that the health authorities be involved by making recommendations, but it was generally agreed that they should not be the final, independent decision-maker.

[2] Interestingly, this is a close reflection of the manner in which health priorities are currently established, in that Health Canada administers and creates regulations that comply with the federal Canada Health Act. This, however, does not concern the privacy of personal information (which, as demonstrated above, is governed by provincial legislation, as well as the federal Privacy Act and PIPEDA)

Others

Although not specifically prompted, several individuals suggested alternative entities that might be best suited to privacy policy development. These suggestions largely focused on health care provider organizations, such as the College of Physicians and Surgeons and the College of Pharmacists, either independently or in conjunction with the government. It was argued that effective policy would emerge out of a collaborative, evidence-based policymaking process in consultation with privacy professionals and health care providers and organizations. Two participants suggested that this mixed approach be taken with a dedicated five- or ten-year timeline for review to ensure relevance.

Conclusion

Overall findings from the discussions about privacy policy and policy setting suggest that there are significant knowledge gaps and poor confidence in existing political processes related to personal information sharing in the health context. Although awareness of legislation concerning data privacy is high, few were able to name the legislation. This ambiguous awareness did not lend itself to a fruitful discussion about the strength of the legislation and the effect of the legislation on the provision of quality care. Furthermore, there was little agreement about who should be responsible for setting policies related to data privacy. I argue that this knowledge deficit is harmful to individuals. Having at least some knowledge of the legislative regimes that govern the flow of information and the manner in which they come to bear upon information sharing and information privacy rights is valuable for individuals, especially in understanding how those rights can be compromised. It also perpetuates the status quo whereby citizens remain uninvolved in many legislative processes because they are thought to lack knowledge on the topic. Encouraging citizen participant in the development of policies and reforms would therefore close some of the knowledge gaps that exist among the public, while also resulting in policy that reflects the preferences and attitudes of those to whom the policy relates.

5.3.2. Informational (Dis)Continuity of Care

A key component of the focus groups was an exploration of perceptions about and experiences with informational continuity of care. We sought to identify participants'

baseline interpretations of current information sharing practices in relation to their preferences for information sharing. The topic was discussed in the context of medical information quite broadly, as well as information sharing preferences in the particular context of ADEs.

The Experience of Siloed Communication

At the beginning of each focus group, participants were asked what information sharing they believed occurred in the event that they were to experience an issue with a medication (i.e., an ADE). This question was aimed at understanding both participants' experience with ADEs and their perceptions about current information sharing practices in the context of ADEs. Comments about ADE experiences and related informational continuity of care were also a common, naturally recurrent theme throughout the sessions. Therefore, the approach to coding for these perceptions included statements that articulated beliefs and experiences beyond those that emerged in response to the question. Out of the coded data, the theme of variability in information sharing began to emerge, articulated through both experiences and beliefs. In some instances, this perspective was taken explicitly. For example, Participant 15 described having had variable experiences with information sharing: "I do believe in continuity of care, including [between the] emergency department and medicine. Did not happen for me." They later noted that information will go their general practitioner (GP), but they have to specify if it is to go to a specialist. Their comments illustrated firsthand how experiences with information sharing varied. Similarly, Participant 8 provided the following statement regarding experiences with information sharing:

> It depends on the physicians. I'm really lucky, I have an amazing GP who's very proactive and the 3 specialists that are involved, they all talk to each other. They all connect. I'm really lucky. I'm very lucky and I understand that that does not happen very often. That was not my previous experience at all.

Others, however, were implicit in their positioning. Participants discursively constructed their experience with informational continuity of care as one that may or may not be representative of the reality of information sharing. They seldom employed absolute statements to describe their experiences with or perceptions about information sharing: "the people to whom I go for one medical event or another *don't always* share the information" (Participant 12); "It's really easy for your GP to forget to tell your specialist…And I think that happens *frequently*." (Participant 13); "I know *my particular*

doctor; it doesn't get outside his walls" (Participant 9). This linguistic positioning suggests that these participants acknowledge the variable reality of informational continuity of care.

Many of the participants spoke of informational continuity of care in the context of their GPs and specialists, yet what was absent from these discussions was the impact of not having a regular GP. Although 85% of British Columbians do have a GP, the remaining percentage must seek care in clinics, seeing different doctors and perhaps even going to different clinics each time (Statistics Canada, 2014). It is likely that these individuals face even greater challenges related to informational continuity of care in the absence of consistent care providers and information sharing across clinics. Overall, the topic of information sharing, addressed frequently in the sessions, elicited comments that reflect the contextuality of information sharing practices and the reality of the fragmented, siloed communication that occurs across care providers more broadly. These shortcomings may be understood instead as informational *discontinuity* of care.

The Role of the Patient

In the groups, another emergent theme related to information sharing practices that touches upon informational discontinuity of care was the role of the patient. Many participants suggested, unprompted, that they ensure (in varying capacities) that all their care providers are made aware of any of their medical events, tests, and so on. For example, Participant 1 noted: "I make sure that whatever tests that I have done, or whatever events happen to occur – medical events – I make sure that everyone is copied on the list – all my specialists." Some detailed their habits of maintaining personal records of all the medications they are taking, including details related to dispensation and beyond. Participants 3 and 9 noted that they both regularly carry their lists with them at all times. Participant 9 in particular took theirs out of their pocket during the session to illustrate, stating "I always have one with me. You never know."

A significant question that emerges here is whether this sense of agency is the product of a desire to be involved in their own care, or a result of poor confidence in the adequacy of current information sharing practices. Most statements surrounding agency do not clearly demonstrate the drivers for this behaviour. Some, however, are a reflection of one case or the other. For instance, Participants 1 and 8 were discussing their 'my eHealth' account, which allows BC residents access to their lab results online,

of which Participant 8 stated “Oh I love it.” Actively using this patient portal suggests that these participants have a keen interest in their own involvement in their circle of care. On the other hand, Participant 3 noted:

> ...before I leave emergency I get them to give me a copy of the emergency thing, because I find that’s the only way I can make sure that the next doctor I see is going to know – or pharmacist or anybody – that’s the only way I can feel comfortable with knowing.

This statement points to a lack of faith in the adequacy of existing informational continuity of care practices.

What is also interesting in the context of this finding is the contrast between either the desire or need for patient agency relative to the status quo whereby patients are relegated to the sidelines in formal policymaking and information sharing regimes. As was noted earlier, patients are often implicated actors in the context of their own information flows and privacy. These findings suggest that the formal structures should be amended to reflect the reality of patient roles that currently exist. Some patients want to have information shared and have greater access to information about their health, yet the current governance structure do not always enable this.

Communication Enables Positive Health Outcomes

Although we cannot conclude with certainty the drivers for this behaviour, we did find that many felt improved communication would have a positive effect on individual health outcomes. Some participants provided fictional scenarios under which information sharing would be essential to their health outcomes. For example, Participant 8 stated that if they had a seizure disorder, they would want to be confident that all their care providers had access to the medications that they take to manage it. Others described firsthand experiences with the consequences of poor information sharing. In the context of ADEs, Participant 1 described their father-in-law’s ADE experience whereby his medications were exacerbating existing violent tendencies that were a symptom of his dementia. Participant 1 explained that the poor communication about this symptom among the patient’s circle of care negatively affected his disease trajectory, incurring unnecessary costs for the health system, and producing a profound emotional impact on the patient and his family. This participant’s father-in-law’s experience demonstrates that the consequences of poor communication are experienced in multiple ways among different actors.

Generally, participants expressed a strong desire for informational continuity of care to enable better health outcomes. This finding is supported by one of the public opinion surveys, which found that 83% of Canadians agree that it is difficult for health care professionals to provide quality care without timely and easy access to their patients' information (Ipsos Reid, 2012). The perceived benefits of enhanced access to patient information is an important driver of liberal information sharing attitudes among patients. In recognition of the perceived benefits of information sharing, individuals do not hesitate to share their information (Whetton, 2013).

Methods of Information Sharing

When asked their preferred method to achieve adequate information sharing, many expressed support for the use of ICTs. Electronic communication was perceived as quick, easy, and practical. It was noted that electronic information sharing is more environmentally sustainable and difficult to lose. Survey results align with the positive perception toward the use of computers for documenting and sharing health information, as 79% of Canadians agreed that they were comfortable with this (Ipsos Reid, 2012). Focus groups participants elaborated, however, that electronic sharing should never be the only method possible. Indeed, some felt that an exclusive reliance on electronic information sharing could be threatened by hacking or a system failure. Participant 17 noted, for example, that Vancouver's location in an earthquake zone introduces the possibility of data loss due to the failure of telecommunications systems during a seismic event. As such, participants noted that there should always be the option to make a telephone call, that there should be electronic and paper-based back-ups of information, and that electronic systems should be protected from hacking.

Patient-Care Provider Trust

The information sharing preferences of focus group participants were, however, largely contingent upon individual interpretations of the circle of care and therefore who should be granted access. For example, one group agreed that pharmacists should have access to information, but there was debate surrounding whether these information sharing privileges should be extended to pharmacy assistants. They also debated this issue in relation to non-medical and non-nursing caregivers (e.g., care aides) in long term care facilities and to allied health professionals (such as physiotherapists or social workers). They concluded that their comfort would be largely contingent upon the level of

professional training that these groups have received, and whether sharing of medication information is deemed necessary in the context of the type of care a patient was receiving (e.g., it was suggested that physiotherapists would not need access to medication information for their work, whereas pharmacists' assistants would).

A significant thematic element that underpins this aspect of the discussion is the implicit trust between health care providers and patients, and specifically the trust patients place with health care providers to keep their personal medical information secure and confidential. Levels of trust in different actors with access to health information were also assessed among Canadians. The survey found that any type of care provider received higher trust ratings compared to any other group, such as health researchers in different arenas, health departments, and insurance companies (Ipsos Reid, 2012). Trust among family doctors was highest, with 83% of Canadians providing trust ratings of 5, 6, 7 on a seven-point scale (where 1 was no trust at all and 7 was great deal of trust) (Ipsos Reid, 2012).

Two focus group participants noted that beyond nurses and doctors, they would like to know who has access to their information and what they were doing with it. Participant 20 summarized this perspective by stating, "So you want the information with those people who can help you if you're in need but you don't want it with those who aren't going to be in that position." It was generally agreed that employers and colleagues should not have access to medical information. The survey results were consistent with our findings. This may be illustrative of the perceived value of medical information, in the sense that it is something deserving of protection because it has the potential to harm in the wrong hands. Interestingly, however, in the 2012 survey, 60% of Canadians agreed that there are few other types of personal information more deserving of legal privacy protection than health information, which was a decrease of 4% from 2007 (Ipsos Reid, 2012).

In this discussion, focus group participants and survey respondents are aligned with positions on the dimensions of privacy described in Chapter 2 in the context of health information. Focus group and survey responses are consistent with a normative construction of privacy that conceptualizes it in terms of degrees of access, wherein the prescriptive power of privacy rests in its capacity to advance other values.

In Consideration of Stigma

Opinions related to information sharing preferences and comfort became more convoluted when the participants in groups A and C considered information sharing in the context of mental illness. In group A, when contemplating sharing different types of information in different contexts, one participant shared that they live with a chronic mental illness for which they take medication. The participant described how their information sharing preferences might change depending on the stability of their mental condition. Of note, they stated that in the event that they were stable, then information sharing should be limited to medication type, whereas when they are unstable they would prefer increased information sharing, including their diagnosis, in the interest of their safety and the safety of others. This reinforced the notion of enhanced informational continuity of care and permitted a unique perspective that others had not yet considered. For example, Participant 3 stated:

> It's interesting just to hear [them] speak because what we're dealing with is our very vanilla type things, I mean, when you hear about something like this. We're not in that loop and we don't really understand.

Others expressed concern about the release of information related to mental illness and the use of medications to treat mental illness (such as antidepressants), among employers and coworkers due to the possibility of stigma. Beyond employers and colleagues, the risk of stigma was discussed in an unexpected way. One participant recounted an instance where a Canadian woman was denied entry in the United States because she was perceived to be a high risk individual due to a previous suicide attempt in which she called 911 and was brought to hospital. The participant was unable to recall the details of the incident, but further research uncovered a highly interesting case that speaks to issues of classification, stigma, and informational inequality. US border agents do have access to police records, but they are not supposed to have access to medical records. This raised a number of questions in the case of the individual that was denied entry to the US. Their case was therefore brought to Ontario's Information and Privacy Commissioner, Ann Cavoukian (CBC News, 2013). Cavoukian (2014) launched an investigation that uncovered a number of similar cases that were a result of questionable data collection and sharing practices in the context of suicide attempts when they led to a call to emergency services. At that time, Toronto Police Services were obligated to record all suicide attempts they responded to, which was then uploaded to the Royal

Canadian Mounted Police's (RCMP) national law enforcement database, the Canadian Police Information Centre (CPIC). Under an agreement with the US Federal Bureau of Investigation (FBI), the CPIC database was then shared from the RCMP to the FBI, which, in turn, granted access to border agents through US Homeland Security (Cavoukian, 2014). Unlike other municipal and provincial police forces that were permitted to use independent judgment in the recording of these cases, the Toronto Police were obligated to do so even in suspected cases (Cavoukian, 2014). The following year, Toronto Police Chief Mark Saunders announced that changes had been made in conjunction with the RCMP that would block border agents' access to certain information in the CPIC and reduce the time of retention and the period to re-evaluate records from five years to two (Gillis, 2015). Following the change, an audit of the database resulted in the removal of almost 65% of existing records (Gillis, 2015). The focus group participant that mentioned this case did not identify the full details of the incident, but rightly believed that this type of government access to medications (and health records) should not be permitted.

The discussions related to mental illness and stigma may be more broadly applicable to such illnesses as HIV/AIDS and other stigmatized conditions. This speaks to van den Hoven's (2001) notion of informational inequality, whereby harm emerges when information is not maintained within its proper sphere, as well as Reiman's (1995) extrinsic and intrinsic losses of freedom, whereby behaviours and attitudes are modified to conform with the status quo out of fear of the consequences of being different. Yet it also illustrates that the problem applies more broadly, even to individuals that may not actually live with a stigmatized illness, addressing issues of classification under otherwise normal circumstances. In particular, Cavoukian's (2014) report revealed a case of a lawyer that had accidentally swallowed a large dose of pills, who then called emergency services. This event was recorded in the CPIC per Toronto Police Services protocol, even though it was accidental. This individual was then questioned by border agents regarding the incident when he tried to cross the border into the US some time afterwards (Cavoukian, 2014). This incident is demonstrative of the problems concerning identity, stigma, and classification in the context of individuals who perceive that they have 'nothing to hide'.

Conclusion

In sum, participants' experiences with informational continuity of care have been varied. In the absence of effective communication and information sharing, many patients take it upon themselves to fill in the gaps. It is unclear whether this is out of a desire to be involved in the circle of care or due to poor trust in the system to appropriately share information. The trust that exists between patients and health care providers to maintain the security of information informs a strong desire for liberal information sharing among one's circle of care. The belief that better information sharing would produce better health outcomes, in both the context of health care broadly and of experiences with ADEs, was expressed by focus group participants, which echoed earlier survey findings. Generally, it was argued that ICTs are best suited for achieving this enhanced information sharing. Many participants, however, were brought to reconsider and re-evaluate their positions in light of more stigmatized positions. In the context of *ActionADE*, these findings point to a strong level of support for our platform from a clinical care perspective.

5.3.3. The Secondary Uses of Health Data and Consent

ActionADE is being designed primarily in the interest of enabling informational continuity of care to improve patient outcomes. The data collected, however, could be employed for future research-based uses. As such, a series of questions in the focus groups addressed the issue of consent and other approaches to managing the introduction of novel information-based harms. Consent was conceptually framed as asking permission for data use. The discussions about consent began with questions about information sharing for care purposes only, then research only, and lastly participants were asked to share their views about the use of their information for both care and then research (i.e., the secondary uses of health data). We ensured applicability to *ActionADE* by explicitly asking about prescription medications in this context. To minimize bias in responses, we did not reveal existing consent requirements that are enshrined into BC's legislative regimes (which few, if any, participants were aware of given the limited familiarity with existing legislation).

Given the strong preference for information sharing among the circle of care, it is unsurprising that participants felt that information sharing among care providers should

be relatively uninhibited. There were no participants who stated that they should be asked permission each time their information was shared among their care providers. Several noted that consent requirements in this context would be detrimental, by creating duplication and adding bureaucratic burden. Recognizing the benefit of liberal information sharing in care contexts, Participant 19 stated:

> …when [you're] in [an emergency] situation you're already not thinking straight, and then they come and ask you what medication are [you] taking, and it's like, oh come on, you got a computer, look it up.

Several other participants expressed favourability toward an opt-out model, whereby individuals are afforded the opportunity to withdraw information sharing privileges at their discretion. In one group, this elicited some debate, arguing on the one hand that it should be an individual's right to opt out, and on the other that it would be detrimental to the individual. These findings are further illustrative of the implicit patient-care provider trust that underpins much of an individual's interaction with the health care system, demonstrating that patients see the value in information sharing and trust their care providers to share information responsibly, thereby eliminating the need for consent.

Liberal information sharing opinions were not always extended to research purposes, in reference to data collection for research, care and research, and research about prescription medications. Participants expressed variable opinions about whether they should be asked each time their information was being used after being collected initially for research purposes. Roughly half of the participants believed that they should only be required to provide consent the first time data is collected for research, while another half felt that they should be asked each time the data was used. Participant 7, who had argued that consent in care would create red tape, reiterated their position in this context:

> As far as I'm concerned, once you've given that survey, that survey is their property. And it goes back to what you said, it creates such red tape and all this other stuff and now they have to go back and contact you again. It'll put things at a standstill.

For the most part, opinions were highly nuanced, indicating contingencies surrounding the type of information being sought and whether it was anonymized. Those who expressed comfort with the future use of their information without the need for

permission tended to do so under the condition that they could not be identified. “If you’re identified, then I believe you should consent. But if you’re not identified, and all personal markers are removed, then fine” (Participant 8). Others advocated for an opt-in/opt-out approach, whereby consent is given at the outset, with the capacity to withdraw consent at any time.

Concerning consent for the secondary uses of health data, responses tended to gravitate toward anonymization and/or an opt-in model of consent. Only one participant stated that they would want to be asked to provide consent each time, stating: “Yeah, you should always consent.” (Participant 13) There were also some participants that articulated that they would not need to be asked permission for information sharing for care and research. Similar to the question about only research uses, however, many expressed more nuanced opinions. The opinions reflected preferences for anonymization or informed consent requirements at a single point in time at the outset:

> I wouldn’t want to be asked every single time someone wanted to access the body of data from the provincial database that was used for my care. If I sign a form saying yes this information is to be used for research in the future, or education actually, I give consent. (Participant 15)

Some stated that it would be dependent upon who was doing the research and why, although one participant argued that the beneficial aspects of research would overshadow any possible negative outcomes: “…if it’s going to affect you in a positive way…you wouldn’t care whether it was anonymized or not at that point in time. You’d be getting the benefit.” (Participant 12). These findings reflect public opinion survey findings as well. Whereas support for the use of EHR data for health research was quite high when it was not specified whether the individual would be identifiable (80% support), this increased to 88% support if information were anonymized (Ipsos Reid, 2012). Furthermore, when given a scenario whereby health records are linked to other records for health research with consent, total support was 69% (Ipsos Reid, 2012).

When explicitly asked about opinions on consent in relation to research about pharmaceutical use, similar concerns were mentioned. One group agreed that it would depend on the medication, who was conducting the research, and what the research was about.

> Generally, I’m comfortable, for example when it comes to medical use. I’m comfortable with sharing that – the medication information on

> cardiac issues. Some other issues, like a member of my family is on mental health drugs – not so sure. (Participant 17)

Much like the discussion on informational continuity of care, there appeared to be a shift in perceptions about consent when considered in the context of mental illness. For instance, Participant 17's quote above reinforces the social sorting that emerges out of classification. Although not explicitly articulated, this discussion about mental illness and the appropriateness of information sharing in these contexts points to the emergent theme of the symbolic and discursive construction of the self through stigmatization. The groups alluded to issues of classification and stigma, yet we see again that they fail to recognize the potential consequences of the ways that they may be classified.

Indeed, my assumption upon beginning this undertaking tended to err toward a similar opinion, in which those who may be considered vulnerable populations (e.g., individuals with mental illness, etc.) would have a preference for greater agency over and stronger protections for their information and the way in which it is managed. This viewpoint emerged out of a concern for stigmatization and social sorting. In this sense, my bias led me to believe that individuals who experience a condition for which they might be stigmatized would prefer an opt-out model of consent, whereby they could withdraw information sharing privileges at their discretion. A unique outlier emerged in discussions on the proposed strategy for opting out of information sharing and my assumptions were proven wrong. Participant 4, who had discussed their mental illness with the group, expressed uncertainty regarding their comfort with an opt-out model (noted earlier). In particular, they suggested that if they were in an unstable mental state and were not taking their medication, inadequate information sharing because of a prior opt-out decision could be dangerous to both themselves and others. This example, then, leads me to highlight the need for privacy protection as long as it does not impede patient safety and quality outcomes.

Overall, the focus groups pointed to the contextuality of consent. Due to high levels of trust between patients and care providers, as well as the tangible benefits of informational continuity of care, minimal consent requirements were preferred in care contexts. There was less agreement about how consent should be managed in research contexts. It is clear that consent is preferred at the point of information collection, but for future uses of data, preferences were spread across the need to re-consent, anonymization, and the capacity to withdraw consent. Consent in instances of data

collection for care as well as secondary, research-based uses were similar. Additional considerations relate to the researcher and the topic of the research.

5.3.4. Privacy & Security

The focus groups addressed a series of questions related to data privacy and security. Participants were asked to describe how secure they perceived their confidential medical information to be in health care facilities and with the government. Perceptions regarding the effectiveness of de-identification were gauged as well. Lastly we asked about participant's awareness of recent breaches of confidential medical information and the effect of this knowledge on their willingness to share information with care providers and the government.

Security of Information in Medical Facilities

Perceptions of the security of confidential medical information in medical facilities were not positive. Many noted that if someone wished to access their information (either within the facility or through hacking) they likely could. It was also mentioned that information is only as secure as the individuals that are handling it, and that this is an inherent risk. Only three participants articulated moderate confidence in the security of their information, citing trust in their doctor's office in keeping information secure and that most professionals receive training on the maintenance of the security of information. These findings are interesting when considered in the context of findings from public opinion surveys. In 2012, although 82% of Canadians indicated that they felt their information was at least moderately safe and secure, there were some obvious uncertainties related to the safety and security of health information as only 41% reported that it was definitely safe and secure (Ipsos Reid, 2012). This suggests that many Canadians have doubts regarding the true security of their medical information.

Security of Information with the Government

Perceptions about the security of confidential medical information in the hands of the government were less consistent. After being told about the information sharing requirements in Vanessa's Law, participants were asked how secure they thought their confidential medical information would be with the federal government. Responses were variable and the complexity of the issue was acknowledged. Some, for example, felt that

it would depend on a number of other factors, such as the extent of dissemination of information after collection and the company that would be contracted to house the data. Similarly, one participant felt they could not comment due to the scope of stakeholders involved: “Who the hell knows…There’s so many fingers in the pie” (Participant 9). Few explicitly expressed the belief that their information would be secure, but it was noted on more than one occasion that they would have no issues as long as the data were anonymized. Participant 11 stated: “I have trouble imagining what circumstances would make it problematic for me.” Lastly, on the other end of the spectrum, one participant expressed skepticism toward the government’s capacity to keep personal information safe and secure, saying that they did not trust easily.

Recognizing Human and Non-Human Actors

Interestingly, the narratives that emerged surrounding informational privacy and security focus largely on the human actors involved in handling the data, rather than the non-human, technical actors that mediate the flow of information. This absence may be interpreted in a number of ways. First, we may consider that the participants either did not fear or did not consider the potential disruption that technologies impose upon privacy, despite this narrative’s prominence in public discourse surrounding ICT development and introduction. From a theoretical perspective, this represents a socially constructivist stance, focusing disproportionately on the human actors involved. This contributes to another dimension of the participant’s inability to recognize the consequences of their own classification, by failing to recognize the construction of the self through technologies.

In another sense, however, it may have been a result of the participant’s inability to conceptualize the ways in which they may effect change related to technologies, viewing human behaviour as something that is easier to modify instead. This may be interpreted as a deterministic stance, whereby the agency of technologies is beyond the control of the human actors that interact with and produce them. Practically speaking, both perspectives suggest that the protection of information is equally contingent upon quality system design as well as proper information handling practices.

Anonymization & De-identification

Despite skepticism toward the capacity of care facilities and government to maintain the privacy and security of data, many participants agreed that anonymizing their data would afford them some protection. Prior discussions related to issues of consent substantiate this finding through the preference of data anonymization to circumvent consent requirements. Anonymized data is that which is altered to make it impossible to link individuals with their data (Safran, et al., 2007). De-identified data is achieved through the removal of identifying information (Council of Canadian Academies, 2015; El Emam, Jonker, Arbuckle, & Malin, 2011; Safran, et al., 2007). Anonymization and de-identification are often employed to circumvent the problematic elements of surveillance and the secondary uses of health data. From a care perspective, some participants discussed a challenge with anonymization in that the usefulness of the data would be compromised. One participant did, however, note that anonymization would not impede upon usability for public health purposes. Aside from usability, there were no other critical perspectives toward anonymization. Of note, the possibility of re-identification and data linking through triangulation were not raised by participants, although it was not explicitly included in the discussion guide either. Unfortunately, however, re-identification through the triangulation of different indicators across data sets is an issue. There is a well-cited example that illustrates the possibility of re-identification, whereby the health record of the former Governor of Massachusetts was identified by matching certain data fields with the Cambridge Voter Registration list (El Emam, Jonker, Arbuckle, & Malin, 2011). Of note, however, one systematic review found that most data re-identification was done by researchers to illustrate the possibility and risk, rather than demonstrating real-life instances (El Emam, Jonker, Arbuckle, & Malin, 2011). Regardless, the focus group findings suggest low awareness of or concern for the possibility of data linking in the current context.

Data Breaches

We did not ask participants whether they had personally experienced a data breach, and none were noted unprompted. Participants were asked about whether they had heard of any recent breaches of medical information in the news, and a small portion of participants were able to identify several breaches of differing levels of severity. Some discussed internal breaches, such as nurses chatting in the hallway and cafeteria about patients, or administrative staff inappropriately accessing the information

of celebrities. Breaches of Canadian data by American companies was mentioned as well. Improper disposal of patient files was noted twice, in terms of CDs and storage devices left in the garbage and printouts in dumpsters. One individual also cited 'serious privacy breaches' by the BC government but did not elaborate on the details of this claim. At least one breach was noted in each group, yet most stated that hearing about these breaches would not have an effect on their willingness to share data. In fact, one noted that they would be more concerned about data being entered incorrectly than being subject to a data breach. These results are interesting in the context of a public opinion survey that measured privacy perspectives quite generally, which found that concern regarding the perceived security of health data was reported among only 3% of Canadians, the lowest among all unprompted responses to the question (Phoenix Strategic Perspectives Inc., 2013). Anonymization was recognized as a solution for identity protection in the event of a data breach, although this may impact the usability of the data.

5.3.5. Information Sharing Advantages Relative to Risks

Many of the findings from the focus groups support the notion that perceptions about the value of informational continuity of care exceed perceptions about the possible negative outcomes of information-based harms. Although participants articulated an awareness of the risks of privacy breaches and that the security of their information could not be guaranteed, most felt that these conditions would not adversely impact their willingness to share their information liberally, especially among the circle of care. For example, Participant 8 stated:

> I would rather lose some of my privacy and have my GP - my specialist, oncologist, whatever – know what's going on and all of them have the report…to me, that quality of care through information is more important than my privacy.

It is particularly interesting, however, that some believed that their perspectives would not be shared among individuals with stigmatized illnesses. Although not explicitly articulated, these perspectives allude to the nothing-to-hide discourse, wherein individuals believe that they have no need to be concerned about the inappropriate use, sharing, and disclosure of their information because their health statuses and medical conditions fall within the 'norm' (Solove, 2011). The consequences of classification were

only considered when it was discussed in terms of those who were believed to have something to hide. As noted in Chapter 2, this perspective is flawed. The individual who was denied entry into the US, for example, and those who face stigma and discrimination in other ways, experience the negative consequences of social sorting and classification, which are often not shared by individuals who do fit neatly within classificatory frameworks, or can be classified in ways that do not typically lead to informational harm. Through the belief that they have nothing to hide, participants fail to recognize and acknowledge the consequences of their own classification. I therefore argue that this dichotomous construction of identity that delineates the normal and abnormal may play a role in participants' relatively liberal information sharing preferences in the context of their care and research.

5.4. Mapping the Balance between Information Sharing and Protection

At the heart of much of this undertaking has been an attempt to strike the ideal balance between information sharing for quality care and information protection for the maintenance of privacy. In keeping with the situational analysis methodology, I approached this question through the use of a positional map.

Positional maps are a visualization of the discursive positions that have and have not been taken in the data. Central to this cartographic approach is the rejection of the assumption that individuals hold a single discursive position. In reality, positions are complex and heterogeneous. In recognition of this perspective, the map instead represents the discursive positions, independent of the actors that expressed or articulated them at any given time. This also acknowledges the porousness of positions while demonstrating the silences in the data. The visualization organizes the positions on an x-y axis based upon a spectrum of less to more.

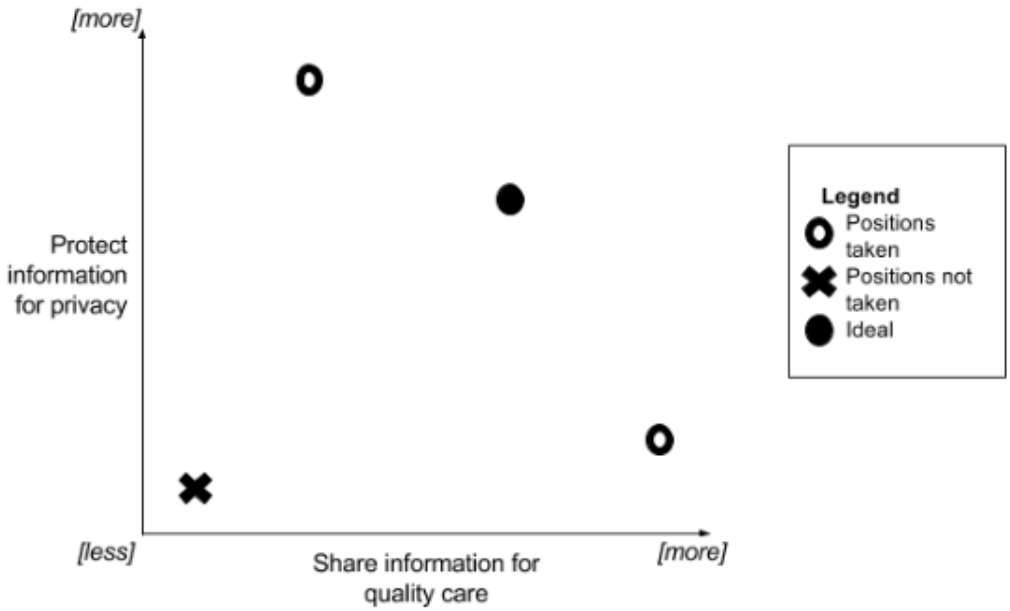

Figure 2: Positional Map of Discourse on Information Sharing Relative to Privacy Protection

Typically, discourse related to the protection of information and sharing information for quality care implies a sacrifice of one in favour of the other (Appari & Johnson, 2010). As illustrated in the map, however, the positions were not absolute. For example, there is often an emphasis on the need for more privacy protection within the confines of the minimal sharing required to achieve quality care. The opposite position is often that strong information sharing is advocated for with a minimal amount of privacy protections. Unsurprisingly, the discursive position whereby both information sharing and protection are low is absent from this context (see the "X" in Figure 2). There is always at least some demand for both, but the demand is often places a greater emphasis on one over the other. The black circle in the positional map indicates the desired balance of adequate information sharing and privacy protection. It is difficult to ascertain whether this balance is achievable in reality, but it is something to strive for.

5.5. Implications for Design (and Beyond)

Although the majority of participants were interested in the informational continuity of care that would be afforded through *ActionADE,* a number of privacy-related recommendations and implications for system design may be drawn out of the feedback

received in the focus groups. The following section will briefly outline the recommended strategies for addressing issues related to care provider access, secondary uses of data, physical security measures, and increasing policy and privacy literacy among the general patient population.

Generally speaking, there are two main strategies employed to protect the privacy of personal health information: the formal conditions of privacy, such as legislation, and the material conditions for privacy, such as the physical and technical conditions that prevent inappropriate access (Reiman, 1995). The privacy policy landscape described above represents the formal conditions of privacy in the context of *ActionADE* and are difficult to change. The physical conditions of privacy include locking doors and cabinets, secure storage of mobile devices, alarms for rooms and buildings, appropriate destruction and disposal of records, and ensuring that records are not removed from the premises (VCH, 2014). Changing the physical conditions of privacy is also largely outside of the scope of the *ActionADE* project, because the implementation sites have pre-existing architectural and procedural standards that govern physical access. In the design of *ActionADE*, there are opportunities to address patient concerns related to privacy through technical measures, which encode social values and norms and produce social implications.

5.5.1. Controlling Access

Participants expressed concern about having certain care provider groups, such as allied health professionals and pharmacy assistants, access their information. Indeed, we found that individuals were less concerned about what type of information was contained in the system, instead expressing concern about who had access to their information. As such, *ActionADE* should include role-based access permissions that are responsive patients desire to authorize or de-authorize access by certain care provider groups (Appari & Johnson, 2010). In the construction of privacy as either access or control, this approach permits a blend of the two dimensions in order to maximize the usefulness of the data while minimizing the imposition on privacy.

The access permissions could mimic existing structures in other health information systems in the province, or they could be developed in conjunction with patients in the future. Other measures identified in existing policies and procedures

include passwords and user IDs, automatic log-off of computers when they are not in use, and encryption (College of Physicians and Surgeons of British Columbia, 2008; VCH, 2014). In order to manage the possibility of a failure of electronic systems, many of our participants recommended that paper-based backups should be available, and that care providers should always have the option to communicate offline. Therefore, in order to ensure informational continuity of care in the event of an interruption in the electronic interface, the implementation of the system may consider printing copies of ADE reports that may be given to patients, faxed to other providers, or stored in paper-based charts. This represents an avenue for future research among patients and care providers in *ActionADE,* wherein the content of the print-outs could be tested among patients to evaluate value, understandability, and so on. Above all, however, it is highly important that these security measures do not interfere with the provision of care.

5.5.2. Anonymize Data

Although *ActionADE* has been designed with a primary interest in clinical functionality, it is also likely that the data collected could be of future use. While many participants called for an opt-out model of consent for the secondary uses of their data, this would be logistically difficult to address due to mandatory reporting requirements in Vanessa's Law and, among academic researchers, complexity emerges in terms of who patients would contact in the event that they wish to opt out. A novel way in which researchers are beginning to manage evolving and contextual consent requirements is through the establishment of systems to support dynamic consent (Spencer et al., 2016). Dynamic consent employs a technological interface that is accessible to research participants, whereby preferences about information sharing and consent can be viewed and changed at any time (Spencer et al., 2016). Although this prototype is not widely available in research settings at this time, and there are still a number of logistical elements that require clarification, it appears to be a solution that would have the capacity to manage the patient preferences that were identified in our findings. In the future, as models of dynamic consent become more sophisticated, the research team may revisit this possibility in the future. In the absence of this model of consent, I recommend that personal information be anonymized and that patients are given the opportunity to provide informed consent at the outset for the secondary uses of their

information contained within *ActionADE*. This may, however, compromise the value of the data as a tool in research.

5.5.3. Training for Care Providers

Patients' concerns regarding the handling of sensitive health information should be addressed at the institutional level as well. Although system designers have little capacity to influence the training and policies concerning information handling at such a broad level, implementation of *ActionADE* could be accompanied by education on the safe handling of information by care providers. This may include briefing on the best way to share and dispose of information collected by and in conjunction with the system, as well as a focus on these practices in the context of stigmatized conditions. This may, therefore, increase patient's confidence in the security of their information, reducing the possibility for treatment avoidance behaviours that were identified in Chapter 3.

5.5.4. Education for Patients

Lastly, I recommend that part of the knowledge translation and dissemination of this project include educational materials and resources for patients to learn more about their informational and privacy rights. Consistent with the recommendations by the OIPCBC (2014) and findings from a systematic review and qualitative undertaking completed by Hill, Turner, Martin, and Donovan (2013), the focus group participants demonstrated a relatively low level of engagement with privacy policy and other safeguards for data sharing and use at present. A consequence of poor awareness of informational rights limits the liberty and autonomy of patients and introduces opportunities for greater information-based harms. I believe that increased patient literacy concerning privacy and policy issues will produce a sustainable impact by shifting patient roles in the policy setting landscape away from implication and toward involvement.

5.5.5. Summary of Recommendations

In sum, I recommend that the following actions be taken to meet the information sharing and privacy preferences of patients in *ActionADE*: 1) develop role-based access controls that manage access based on patient preferences; 2) ensure informed consent

is received at the outset for the secondary uses of *ActionADE* data and then anonymize the data for all future research uses; 3) incorporate educational components on safe information handling practices in the implementation of *ActionADE* for care providers; and, 4) develop a set of educational and resource materials to increase literacy and maintain the sustainability of patient involvement in policy and design decisions. I also recommend that *ActionADE* implement additional technical measures, such as user IDs and passwords, to ensure the security of the system.

5.6. Conclusion

In this chapter, I have presented an analysis of the information sharing and privacy environment in relation to the implementation of *ActionADE*. The findings from focus groups as well as policy documents, public opinion surveys, and relevant literature have been analyzed using Clarke's (2005) situational mapping strategy, thereby providing a nuanced, in-depth, contextual understanding of the scope of the situation. *ActionADE* was first situated within the existing privacy policy environment, explicating the central, marginal, and implicated actors in this policy setting. A social worlds and arenas map was used to visualize the relations between these collectives and the different discourses and artefacts that they contribute to the situation. I then analyzed the focus group findings relationally to explore participant preferences and perceptions about medication information sharing and the policy landscape. This section identified major thematic elements in the discussions and situated them nationally using findings from public opinion surveys. Using a positional map, I then responded to the overarching question of how to balance information sharing and information protection in the context of *ActionADE,* examining the discursive positions that emerged in the previous sections. Lastly, drawing from all the findings, I identified a series of recommendations and implications for the design and implementation of *ActionADE* that may be taken into consideration in order to maximize patient satisfaction with the system and its usability in the policy context.

Chapter 6. Conclusion

This thesis has explored key issues and opportunities in health data and privacy, particularly in the context of *ActionADE*. Through this undertaking, it has been my intention to identify and situate these issues and opportunities in order to mitigate privacy concerns at the outset of the introduction of *ActionADE.* This chapter will provide a brief review of the key arguments and findings of the thesis, identify limitations in the research, and propose directions for further research that builds upon the thematic and methodological aspects of the thesis.

6.1. Review of Thesis

This thesis began by introducing the notion of information sharing and privacy in the development and implementation of ICTs as a balancing act. The two concepts are often articulated dichotomously, yet their real world applications are much more ambiguous and dynamic, particularly in the health domain. In this regard, I discussed privacy and information sharing as a spectrum, featuring a complex range of human and non-human actors, political elements, social norms, and beyond.

This description established the groundwork for the following two chapters. In Chapter 2, I provided context for the development of ICTs in health and outlined a typology for the dominant perspectives from which these ICTs are studied. This culminated in the presentation of the theoretical lens that guided the research. STS principles were essential to the unpacking, situating, and contexualizing of relevant issues that emerged throughout the research project. Through an STS lens that acknowledges the social, technical, and political elements that come to bear on the design and implementation of ICTs in health, I presented a series of key considerations that would be revisited in the context of *ActionADE*. I identify issues related to classification as a key aspect of concern related to privacy.

The concept of privacy was unpacked in Chapter 3. To understand the complexity and messiness of data privacy in relation to the necessity of information sharing in health, I sought to discuss traditional conceptualizations of privacy. To simplify the discussion, I positioned these conceptualizations across three dimensions, consistent with the prolific work in the field of privacy of Helen Nissenbaum (2010).

These dimensions were elaborated upon, identifying parallels in the work of other scholars in privacy, including Daniel Solove (2001; 2002; 2006; 2011). In doing so, I discuss how these conceptualizations are often inadequate for managing the need for simultaneous data sharing and protections in health. This results in the identification of a reconceptualization of privacy through a sociotechnical lens, highlighting the contextuality and importance of privacy issues in health. The proposed reconceptualization was applied to an analysis of focus group data in the development and implementation of *ActionADE.*

6.2. Review of Findings

This thesis examined data collected through focus groups with patients, as well as policy documents, public opinion surveys, and news sources, in order to thoroughly situate *ActionADE* within the complex sociotechnical environment into which it will be implemented. The analysis began with a presentation of the policy environment that will come to bear on *ActionADE*. This was completed through the use of a social worlds and arenas map, which aided in the visualization of the complex network of social worlds that influenced the arena of data privacy in the context of *ActionADE*.

Analysis of the focus group data was enabled by Clarke's (2005) situational mapping strategy, which involved a number of iterations of a mapping process of all of the relevant individual and collective, human and non-human actors, political elements, discourses, values, and more. This iterative mapping process began as a broad, messy enterprise, and eventually resulted in a concise map that enabled the construction of a relational analysis between the different key elements. I focused this analysis on the policy environment, informational continuity of care, secondary uses of health data and consent, and privacy and security of health data. First, the policy landscape was contrasted to patient awareness of the legislative regimes that govern the flow of their information that was uncovered in the focus groups. This demonstrated significant knowledge gaps and opportunities for public education, consistent with other research. The remainder of the key thematic elements were introduced to provide an understanding of the current experiences of and preferences for informational continuity of care, perceptions about the privacy and security of health data, and preferences for consent. For the most part, the focus group findings were consistent with public opinion data. The findings suggested that there was support for the informational continuity of

care afforded by *ActionADE*, and that the value of information sharing often outweighed the possibility of an information-based harm, although the extent to which privacy violations could affect individuals was rarely identified.

The analysis of focus group findings and other policy and news media documents culminated in a study of the discourse relating to the balance of information sharing and protection in this situation. The different discursive positions were identified using a positional map, and that which was absent from the data was identified as well. The map was employed to visualize what may be considered an 'ideal' balance of information sharing and protection, which is not often articulated, but may address the needs of the diverse actors present in the situation. The application of this argument produced a series of recommendations that may be used to inform the design and implementation of *ActionADE,* which would be responsive to the demands and preferences of patients, as well as the constraints of the existing environment. These recommendations are a reflection of the complex sociotechnical reality into which health information systems are implemented.

6.3. Limitations

There are limitations to this research project that must be addressed, some of which apply specifically to the context of this research, while others are product of the methodology more broadly. I will briefly identify and address these shortcomings in this section.

Concerning the structure of the groups, there were certain aspects that affected the study and may be mitigated in the future. First, the discussion on information and privacy laws was significantly impeded by the relatively low awareness of legislative frameworks on the part of participants. Although this in and of itself is an interesting finding, the discussion guide had intended to address the question of whether privacy policies interfere with or enhance clinicians' capacity to provide care. The participants were provided with a short document that outlined some of the legislative structure (Appendix A), but this was done directly in advance of the question in the middle of the session. A more fruitful discussion would have emerged had the participants been afforded more information and adequate time to read it and ask questions. Any future groups held by *ActionADE* should be aware of this shortcoming and therefore ask the

participants to arrive 10-15 minutes early to read the provided information sheet, and then given additional time during the session to reflect on it.

Second, the in-person recruitment in the ED as part of the recruitment strategy was intensive. It demanded a significant time commitment on the part of the researchers to recruit an adequate number of potential participants. The length of time between recruitment and the groups likely contributed to the attrition from these groups, in that individuals who had been recruited first were less likely to participate. Beyond the attrition and intensiveness of the recruiting, it would not have been possible for many other researchers (especially graduate student researchers) to do so in the absence of direct access to this opportunity in VGH through the *ActionADE* project. Therefore, the application of a methodology that includes recruitment among patient populations to a different study that did not have that access would likely not be possible.

Third, there were some focus group participants that participated very little, or not at all. This is a common shortcoming of focus group research in general. A vocal minority often emerged and inadvertently silenced others who may have been introverted to begin with. Future focus groups should make a stronger effort at creating opportunities for those individuals to express themselves to the extent that they so desire. The project may also consider asking potential recruits about their comfort with speaking out loud in a group, thereby eliminating the risk of this occurrence.

Aside from these specific limitations, a broader limitation of focus group research applies here. In particular, the demand for participant self-selection has the potential to bias the sample included in the groups, thereby limiting the generalizability of the groups (Lavrakas, 2008). Although generalizability was not a goal of this project, particularly given the contextuality that has been emphasized throughout this thesis, the self-selection bias may have had an effect on the findings. In particular consideration of the finding related to the patient role in the maintenance of informational continuity of care, it is possible that individuals at a higher likelihood of self-selecting for this research undertaking would also be at a greater likelihood of participating in their own care. In this thesis, the issue of generalizability was mitigated by situating focus group findings in the broader Canadian context through comparison with public opinion surveys.

6.4. Areas for Future Research

Through this thesis, I have identified some areas for future research specifically within the *ActionADE* project. Here, I will elucidate some of these areas and identify other broader areas for future research that would be of value beyond the project.

The application of the above recommendations would be best approached through future research with patients. In particular, the development and knowledge translation and dissemination of educational materials for patients regarding policy should be done with the aid of patients. Patient perspectives would ensure relevance and comprehension of the materials, thereby facilitating uptake. Patient and clinician perspectives on the possibility of print-outs of the *ActionADE* reports must be considered as well. For clinicians, the research team may ascertain the design and content of the reports to maximize clinical value. Giving patients access to their records may require a greater understanding of the value of doing so. The *ActionADE* project has not studied the effect that this would have on patients, and what kind of unanticipated effects may emerge out of this, so it is not considered a firm recommendation at this time. Further research on the effectiveness of similar interventions may be required, which could then inform the development of a printed report that would be useful for patients.

In light of the preliminary findings that emerged in relation to stigma, future research in this project may consider undertaking focus groups among populations with stigmatized conditions. This would provide a useful perspective that was not easily obtained in these groups. Additionally, participants could be presented with scenarios that allude to issues of stigmatization to promote further comment and consideration. Other areas of future research involve the application of STS theoretical constructs, an orientation toward patients, and approaches to reconceptualizing privacy to other technological interventions. Because the research project was situated in Vancouver, it would be interesting to conduct similar studies in other Canadian and international contexts.

6.5. Conclusion

This thesis has made a number of arguments, both theoretically, methodologically, and practically. I have demonstrated that the current conditions of

privacy are not effectively responding to the complexity of the health domain. In response to the inadequate status quo, I argue that potential issues related privacy should be addressed contextually in relation to any given technological undertaking, considering the social reality (e.g., practices related to the disposal of files, consequences of classification), political regimes (e.g., governmental and institutional policies), and technical specifications (e.g., access requirements).

I have also argued that gaining a robust understanding of the social reality includes incorporating implicated actors – in this situation, patients. I have demonstrated that patients' views are often not considered in analytically useful ways, largely solicited through national public opinion surveys, if at all. Although these surveys add value to more in-depth methods, they alone fail to capture the idiosyncrasy of patient perspectives. I have also argued for and demonstrated the value in applying the theoretical constructs found in STS to the *ActionADE* project, which may be extended to the implementation of any technology that involves the collection, use, and transmission of personal information.

In these respects, I have contributed new knowledge on a number of topics and strengthened arguments on others. In the field of privacy, I have rationalized and contributed to the push toward reconceptualizing privacy to meet the unique demands of health contexts. I have made a valuable connection in applying STS concepts to this reconceptualization, and demonstrated its efficacy by analyzing focus group and policy data through that lens. I have also added qualitative patient perspectives toward health information privacy in a field in which these voices are often absent. In doing so, I have increased the robustness of the *ActionADE* undertaking by informing elements of its design and implementation.

At the intersection of data privacy, public policy, and health technologies is a complex network of human and non-human actors with competing demands related to information sharing and protection. As has been demonstrated in this thesis, the introduction of novel technologies to solve gaps in communication must contend with corresponding demands and constraints, oftentimes to the detriment of individual privacy. The ideal balance between information sharing demands and the need for privacy protections are often positioned dichotomously, yet achieving an ideal balance between the two would require that they are treated as complementary. Is it possible for

a novel technology to meet the informational needs of care providers and the privacy preferences and patients, while conforming to the political landscape? Although I have attempted to strike this balance by informing the development of *ActionADE*, the effect of these recommendations remains to be seen, if they are taken up. Furthermore, like any sociotechnical intervention, the unintended consequences will not be immediately visible. Information-based harms are indeed often a result of unintended outcomes that become apparent when technology breaks down. Privacy demands must therefore be considered and revisited throughout the lifecycle of a technological intervention. This thesis has set the stage for appropriate and effective information sharing and data privacy in *ActionADE*, but only through implementation and use will it become clear how well these strategies protect and manage the interests and expectations of patients, care providers, and policymakers.

References

Aarts, J., Callen, J., Colera, E. & Westbrook, J. (2010). Information technology in health care: Socio-technical approaches. *International Journal of Medical Informatics, 76*(6), 389-390.

Angus Reid Public Opinion. (2012, Jun 5). *British Columbians would share depersonalized health care data.* Retrieved from http://angusreidglobal.com/wp-content/uploads/2012/06/2012.06.05_Data_BC.pdf

Angus Reid Public Opinion. (2013, Apr 8). *Canadians comfortable with the public sector using private data.* Retrieved from http://angusreidglobal.com/wp-content/uploads/2008/11/2013.04.08_CityAge.pdf)

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

Auffray, C. & et al. (2016). Making sense of big data in health research: Toward an EU action plan. *Genomic Medicine, 8*(71), 1-13.

Bailey, C., Peddie, D., Wickham, M. E., Badke, K., Small, S. S., Doyle-Waters, M. M., . . . Hohl, C. M. (2016). Adverse drug event reporting systems: A systematic review. *British Journal of Clinical Pharmacology, 82*(1), 17-29.

Balka, E. (2014, Sept 29). Adverse drug events in context: A preliminary overview of systems level issues influencing patient safety. *Presented at C2E2 Rounds*. Vancouver, BC.

Balka, E. & Kahnamoui, N. (2004). Technology Trouble? Talk to Us: Findings from an Ethnographic Field Study. *Proceedings Participatory Design Conference 2004* (pp. 224-234). Toronto: ACM.

Balka, E. & Star, S. L. (2015). Mapping the body across diverse information systems: Shadow bodies and how they make us human. In G. C. Bowker, S. Timmermans, A. E. Clarke, & E. Balka (Eds.), *Boundary Objects and Beyond: Working with Leigh Star* (pp. 417-434). Cambridge, MA: MIT Press.

Barbour, R. (2008). *Introducing Qualitative Research: A Student's Guide to the Craft of Doing Qualitative Research.* Thousand Oaks, CA: SAGE Publications.

BC Auditor General. (2017). *Health Funding Explained 2.* Retrieved from http://www.bcauditor.com/sites/default/files/publications/reports/FINAL_HFE2.pdf

BC Medical Association. (2009). *BC Physician Privacy Toolkit, 2nd Ed.*

BCCLA. (N.D.). *Our History.* Retrieved from BC Civil Liberties Association: https://bccla.org/about/our-history/

BCCLA. (2013, Feb 8). *Privacy groups demand halt to BC ID Card roll-out.* Retrieved from BC Civil Liberties Association: https://bccla.org/news/2013/02/privacy-groups-demand-halt-to-bc-id-card-roll-out/

Ben-Zeev, D., Young, M. A., & Corrigan, P. W. (2010). DSM-V and the stigma of mental illness. *Journal of Mental Health, 19*(4), 318-327.

Berg, M. (2004). *Health Information Management: Integrating Information Technology in Health Care Work.* New York, NY: Psychology Press.

Bernard, H. R. (1995). *Research Methods in Anthropology: Qualitative and Quantitative Approaches* (2nd Edition ed.). Walnut Creek, CA: AltaMira Press.

Bourne, P. E. (2014). What Big Data means to me. *JAMIA, 21*(2), 194.

Boutilier, A. (2016, Jun 24). *Canada's privacy law 'ill-suited' to 21st century, watchdog warns Trudeau.* Retrieved from The Star: https://www.thestar.com/news/canada/2016/06/24/canadas-privacy-law-ill-suited-to-21st-century-watchdog-warns-trudeau.html

Bowker, G. C., & Star, S. L. (1999). *Sorting Things Out: Classification and its Consequences.* Cambridge, MA: MIT Press.

boyd, d. & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological and scholarly phenomenon. *Information, Communication, and Society, 15*(5), 662-679.

Braga, M. (2017, May 19). *Canadians 'reluctant' to accept new police powers, prefer privacy online, government finds.* Retrieved from CBC News: http://www.cbc.ca/news/technology/national-security-consultation-report-findings-green-paper-1.4124543

Budnitz, D. S., Lovegrove, M. C., Shehab, N. & Richards, C. L. (2011). Emergency hospitalizations for adverse drug events in older Americans. *New Englad Journal of Medicine, 365*(21), 2002-2012.

Canada. Parliament. House of Commons. Standing Committee on Access to Information, Privacy and Ethics. (2017). *Evidence*. Meeting 54, April 4. 42nd Parliament, 1st session. Available http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-54/evidence.

Canada Health Infoway. (2014, Oct 20). *Accelerating Clinical Interoperability in Canada: The Path Forward.* Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/2329-accelerating-clinical-interoperability-in-canada-the-path-forward-2/view-document?Itemid=101

Cavoukian, A. (2014). *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC.* Information and Privacy Commissioner.

CBC News. (2010, Jan 4). *HIV travel ban lifted in the U.S.* Retrieved from http://www.cbc.ca/news/technology/hiv-travel-ban-lifted-in-u-s-1.943571

CBC News. (2013, Nov 29). *Canadian woman refused U.S. entry because of depression.* Retrieved from CBC News: http://www.cbc.ca/news/canada/toronto/canadian-woman-refused-u-s-entry-because-of-depression-1.2444960

Chruscicki, A., Badke, K., Peddie, D., Small, S. S., Balka, E. & Hohl, C. M. (2016). Pilot-testing an adverse drug event reporting for prior to its implementation in an electronic health record. *SpringerPlus, 5*, 1764.

CIHI. (2013, June). *Summary and recommendations for moving forward from Better Information for Improved Health: A vision for health system use of data in Canada.* Retrieved September 10, 2016, from https://www.infoway-inforoute.ca/en/component/edocman/1689-a-vision-for-health-system-use-of-data-in-canada-executive-summary/view-document

Clarke, A. (2005). *Situational Analysis: Grounded Theory After the Postmodern Turn.* Thousand Oaks: SAGE Publications.

Clarke, A. E., Friese, C., & Washburn, R. (Eds.). (2015). *Situational Analysis in Practice: Mapping Research with Grounded Theory.* New York, NY: Routledge.

Classen, D. C., Pestotnik, S. L., Evans, R. S., Lloyd, J. F., & Burke, J. P. (1997). Adverse drug events in hospitalized patients: Excess length of stay, extra costs, and attributable mortality. *JAMA, 277*(4), 301-306.

College of Physicians and Surgeons of British Columbia. (2008, February 21). *A Precis to the Data Stewardship Framework: The Transition to EMRs.* Retrieved May 2, 2016, from https://www.cpsbc.ca/files/pdf/PSG-Data-Stewardship-Precis.pdf

Council of Canadian Academies. (2015). *Accessing Health and Health-Related Data in Canada.* Retrieved Sep 14, 2016, from http://www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/Health-data/HealthDataFullReportEn.pdf

Daly, J. (1989). Innocent murmurs: Echocardiography and the diagnosis of cardiac normality. *Sociology of Health & Illness, 16*(1), 62-80.

Denham, E. (2015). *Examination of British Columbia Health Authority Privacy Breach Management.* Office of the Information and Privacy Commissioner for British Columbia.

Department of Finance Canada. (2011). *Canada Health Transfer.* Retrieved from Government of Canada: https://www.fin.gc.ca/fedprov/cht-eng.asp

El Emam, K., Jonker, E., Arbuckle, L. & Malin, B. (2011). A systematic review of re-identification attacks on health data. *PLoS One, 6*(12), e28071.

Fairchild, A. L., & Bayer, R. (2016). In the name of population well-being: The case for public health surveillance. *Journal of Health Politics, Policy and Law, 41*(1), 119-128.

FIPA. (2013a). *BC Government's ID Card 'consultation' literally won't take no for an answer.* Retrieved from BC Freedom of Information and Privacy Association: https://fipa.bc.ca/b-c-governments-id-card-consultation-literally-wont-take-no-for-an-answer-4/

FIPA. (2013b). *The BC Services Card, and why you should be concerned about it.* Retrieved from BC Freedom of Information and Privacy Association: https://fipa.bc.ca/the-bc-services-card-and-why-you-should-be-concerned-about-it/

FIPA. (2014). *2014 Annual Report.* Retrieved from BC Freedom of Information and Privacy Association: https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/FIPA-Annual-Report-2014-FINAL.pdf

FIPA. (2017). *What we do.* Retrieved from BC Freedom of Information and Privacy Association: https://fipa.bc.ca/about-us/what-we-do/

Foucault, M. (1975). *Discipline & Punish: The birth of the prison.* Paris: Editions Gallimard.

Fried, C. (1968). Privacy. *The Yale Law Journal, 77*(3), 475-493.

Gavison, R. (1980). Privacy and the limits of the law. *The Yale Law Journal, 89*(3), 421-471.

Gillis, W. (2015, Aug 17). *Toronto police curb disclosure of suicide attempts to US border police.* Retrieved from The Star: https://www.thestar.com/news/crime/2015/08/17/toronto-police-curb-disclosure-of-suicide-attempts-to-us-border-police.html

Glaser, B. G. & Strauss, A. L. (1967). *Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine Publishing Company.

Government of British Columbia. (N.D). *BC Services Card: Adults who drive*. Retrieved from Government ID: http://www2.gov.bc.ca/gov/content/governments/government-id/bc-services-card/the-card-for-you/adults-who-drive

Grande, D., Mitra, N., Shah, A., Wan, F., & Asch, D. A. (2013). Public preferences about secondary uses of electronic health information. *JAMA Internal Medicine, 173*(19), 1798-1806.

Greenhalgh, T., & Stones, R. (2010). Theorising big IT programmes in healthcare: Strong structuration theory meets actor-network theory. *Social Science & Medicine, 70*, 1285-1294.

Gurwitz, J. H., Field, T. S., Harrold, L. R., Rothschild, J., Debellis, K., Seger, A. C., . . . Bates, D. W. (2003). Incidence and preventability of adverse drug events among older persons in the ambulatory setting. *JAMA, 289*(9), 1107-1116.

Haggerty, J. L., Reid, R. J., Freeman, G. K., Starfield, B. H., Adair, C. E., & McKendry, R. (2003). Continuity of care: A multidisciplinary review. *BMJ, 22*, 1219-1221.

Hanseth, O., & Monteiro, E. (1997). Inscribing behaviour in information infrastructure standards. *Accounting, Management, and Information Technologies, 7*(4), 283-311.

Hazell, L., & Shakir, S. A. (2006). Under-reporting of adverse drug reactions: A systematic review. *Drug Safety, 29*(5), 385-396.

Health and Human Services. (2014). *Health Information Privacy Law and Policy*. Retrieved from HealthIT.gov: https://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy

Health Canada. (2017, Feb 17). *Canada Reaches Health Funding Agreement with British Columbia.* Retrieved from News Release: https://www.canada.ca/en/health-canada/news/2017/02/canada_reaches_healthfundingagreementwithbritishcolumbia.html

Hill, E. M., Turner, E. L., Martin, R. M., & Donovan, J. L. (2013). "Let's get the best quality research we can": Public awareness and acceptance of consent to use existing data in health research: A systematic review and qualitative study. *BMC Medical Research Methodology, 13*(72), 1-10.

Hohl, C. M., Lexchin, J. R., & Balka, E. (2015). Can reporting of adverse drug reactions create safer systems while improving health data. *CMAJ, 187*(11), 179-180.

Humer, C., & Finkle, J. (2014, Sept 24). *Your medical record is worth more to hackers than your credit card.* Retrieved from Reuters: http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Ipsos Reid. (2012). *What Canadians Think: Electronic Health Information and Privacy Survey 2012.*

Jenkins, G. M. (2004). A qualitative study of women's views on medical confidentiality. *J. Med. Ethics, 31*, 499-504.

Kaplan, B. (1995). The computer prescription: Medical computing, public policy and views of history. *Science, Technology and Human Values, 20*(1), 5-38.

Kruse, C. S., Goswamy, R., Raval, Y., & Marawi, S. (2016). Challenges and opportunities for big data in health care: A systematic review. *JMIR Medical Informatics, 4*(4), e38.

Lavrakas, P. (2008). *Encyclopedia of Survey Research Methods.* Thousand Oaks: SAGE Publications Inc.

Lazarou, J., Pomeranz, B. H., & Corey, P. N. (1998). Incidence of adverse drug reactions in hospitalized patients: A meta-analysis of prospective studies. *JAMA, 279*(15), 1200-1205.

Lyon, D. (2015). *Surveillance after Snowden.* Cambridge: Polity Press.

Malin, B. A., El Emam, K., & O'Keefe, C. M. (2013). Biomedical data privacy: Problems, perspectives and recent advances. *JAMIA, 20*(1), 2-6.

Mariner, W. (2007). Mission creep: Public health surveillance and medical privacy. *Boston University Law Review, 87*, 347-395.

Matthewman, S. (2011). *Technology and Social Theory.* New York: Palgrave Macmillan.

McDonald, J., & Swain, D. (2016, Sep 28). *Millions of Canadians don't have to be told if health information breached.* Retrieved from CBC News: www.cbc.ca/news/health/health-records-privacy-breaches-1.3780963

McElroy, J. (2017, Apr 3). *Thousands more affected by PharmaNet breach, government reveals.* Retrieved from CBC News: http://www.cbc.ca/news/canada/british-columbia/pharmanet-bc-vpd-arrest-1.4053795

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy, 39*(3), 411-428.

Nass, P., Levine, S., & Yancy, C. (n.d.). *Methods for involving patients in topic generation for patient-centered comparative effectiveness research: An international perspective.* Research Priorities White Paper, Patient-Centered Outcomes Research Institute (PCORI).

Nebeker, J. R., Barach, P., & Samore, M. H. (2004). Clarifying adverse drug events: A clinician's guide to terminology, documentation, and reporting. *Annals of Internal Medicine, 140*(10), 795-801.

Nissenbaum, H. (2010). *Privacy in Context: Technology, policy, and the integrity of social life.* Stanford, CA: Stanford University Press.

OIPCBC. (2014). *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector.* Special Report, The Office of the Information and Privacy Commissioner for British Columbia.

OIPCBC. (2015a). *Guide to access and privacy protection under FIPPA.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1466

OIPCBC. (2015b). *Guide to B.C.'s PIPA for businesses and organizations.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1438

Peddie, D., Small, S. S., Badke, K., Wickham, M. E., Bailey, C., Chruscicki, A., . . . Hohl, C. M. (2016). Designing an adverse drug event reporting system to prevent unintentional re-exposures to harmful drugs: Study protocol for a multiple methods design. *JMIR Research Protocols, 5*(3), e169.

PHAC. (2008, Apr 4). *History*. Retrieved from Public Health Agency of Canada: http://www.phac-aspc.gc.ca/about_apropos/history-eng.php

Phoenix Strategic Perspectives Inc. (2013). *Survey of Canadians on Privacy-Related Issues, Prepared for the Office of the Privacy Commissioner of Canada.* Final Report, Ottawa.

Price, M., & Lau, F. Y. (2013). Provider connectedness and communication patterns: Extending continuity of care in the context of the circle of care. *BMC Health Services Research, 13*(309).

Reed, G. M., Drescher, J., Krueger, R. B., Atalla, E., Cochran, S. D., First, M. B., . . . Saxena, S. (2016). Disorders related to sexuality and gender identity in the ICD-11: Revising the ICD-10 classification based on current scientific evidence, best clinical practices, and human rights considerations. *World Psychiatry, 15*(3), 205-221.

Reiman, J. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology and Law Journal, 11*(1), 27-44.

Reiman, J. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs, 6*(1), 26-44.

Rivkin-Haas, E. (2011). Electronic medical records and the challenge to privacy: How the United States and Canada are responding. *Hastings International and Comparative Law Review, 34*(1), 177-202.

Safran, C., Bloomrosen, M., Hammond, E., Labkoff, S., Markel-Fox, S., Tang, P. C. & Detmer, D. E. (2007). Toward a national framework for the secondary use of health data: An American Medical Informatics Association white paper. *JAMIA, 14*(1), 1-9.

Sankar, P., Moran, S., Merz, J. & Jones, N. (2003). Patient perspectives on medical confidentiality: A review of the literature. *Journal of General Internal Medicine, 18*, 659-669.

Schrag, S. J. et al. (2004). SARS surveillance during emergency public health response, United States, March - July, 2003. *Emerging Infectious Diseases, 10*(2), 185-194.

Smolina, K., Persaud, N. & Morgan, S.G. (2016). Toward better prescription drug surveillance in Canada. *CMAJ, 188*(11), E252-E253.

Sobeys West Inc. v. College of Pharmacists of British Columbia, 2016 BCCA 41 (BC Court of Appeals January 27, 2016).

Solove, D. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*(6), 1393-1462.

Solove, D. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087-1155.

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

Solove, D. (2011). Why privacy matters even if you 'nothing to hide'. *Chronicle of Higher Education, 57*(37), B11-B13.

Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G. (2016). Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: A qualitative study. *JMIR, 18*(4), e66.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111-134.

Statistics Canada. (2014). *Population with a regular medical doctor, by sex, provinces and territories (Percent).* Retrieved from Summary Tables: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/health76b-eng.htm

Suchman, L. A. (2006). *Human-machine configurations: Plans and situated actions.* New York, NY: Cambridge University Press.

Taylor, J. R., Groleau, C., Heaton, L. & Van Every, E. (2001). *The Computerization of Work: A Communication Perspective.* Thousand Oaks, CA: Sage Publications Inc.

Timmermans, S. & Berg, M. (2003a). *The Gold Standard: The Challenge of Evidence-Based Medicine and Standardization in Health Care.* Philadelphia, PA: Temple University Press.

Timmermans, S. & Berg, M. (2003b). The practice of medical technology. *Sociology of Health & Illness, 25*, 97-114.

Timmermans, S. & Epstein, S. (2010). A world of standards but not a standard world: Towards a sociology of standards and standardization. *Annual Review of Sociology, 36*, 69-89.

Tolar, M. & Balka, E. (2012). Caring for individual patients and beyond: Enhancing care through secondary use of data in a general practice setting. *International Journal of Medical Informatics, 81*, 461-474.

Vallano, A., & et al. (2005). Obstacles and solutions for spontaneous reporting of adverse drug reactions in the hospital. *British Journal of Clinical Pharmacology, 60*(6), 653-658.

van den Hoven, J. (2001). Privacy and the varieties of informational wrongdoing. In R. A. Spinello, & H. T. Tavani (Eds.), *Readings in CyberEthics* (pp. 488-500). Sudbury, MA: Jones and Bartlett Publishers.

VCH. (2012, July). *Caring for Your Information: Notice to our Patients, Clients and Residents.* Retrieved from http://www.vch.ca/Documents/Client-Privacy-Notification-English.pdf

VCH. (2014, March 7). *Information Privacy and Confidentiality Policy.* Retrieved May 2, 2016, from https://www.vch.ca/media/VCH-Information-Privacy-and-Confidentiality-Policy.pdf

Viseu, A. C. (2004). Situating privacy online. *Information, Communication and Society, 7*(1), 92-114.

Warren, S.D. & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review*. 4(5), 193-220.

Westin, A.F. (1967). *Privacy and Freedom.* New York: Antheneum.

Whetton, S. (2013). Personal health information, privacy and surveillance: Do we need a critical voice. *Studies in Health Technology and Informatics, 192*, 234-238.

Whiddett, R. H. (2006). Patient attitudes towards sharing their health information. *International Journal of Medical Informatics, 75*(7), 530-541.

Zed, P. J., Abu-Laban, R. B., Balen, R. M., Loewen, P. S., Hohl, C. M., Brubacher, J. R., . . . Purssell, R. A. (2008). Incidence, severity and preventability of medication-related visits to the emergency department: A prospective study. *CMAJ, 3*(178), 1563-1569.

Zimmer, M. (2015). Privacy law and policy. In R. &. Mansell (Ed.), *The International Encyclopedia of Digital Communication and Society* (pp. 971-982). Wiley Blackwell.

Zinszer, K., Tamblyn, R., Bates, D. W. & Buckeridge, D. L. (2013). A qualitative study of health information technology in the Canadian public health system. *BMC Public Health, 13*(509), 1-7.

Appendix A.

Participant Handout

The Privacy of Your Pharmaceutical Data (In Brief)

Information about your medications is a kind of personal health information. Personal information is legally defined as “recorded information about an identifiable individual other than contact information” (BC Freedom of Information and Protection of Privacy Act, Schedule 1, Definitions). This includes your health information. To follow is an overview of the policy frameworks that pertain to the collection, use, and disclosure of your medication-related information:

Provincially, two main pieces of legislation that govern your pharmaceutical data are the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Information Protection Act (PIPA). Both outline the ways that personal information can and cannot be collected, used, and disclosed, including details about when you must provide consent for these activities and when consent is not required. FIPPA applies to public sector entities, like hospitals and health authorities, while PIPA applies to private sector organizations, like medical imaging laboratories and privately-run doctors’ offices. Both laws also govern the use of data for research purposes.

Other provisions related to the privacy of personal health information are found in other pieces of health legislation, like the Ministry of Health Act and the Public Health Act. While not specifically related to pharmaceutical data, these types of provisions give authority to collect, use, and disclose of information by the Minister of Health, insurers, and so forth. Specific to pharmaceutical information is the Pharmaceutical Services Act, which governs the collection, use, and disclosure of personal information (including medication information) related to paying for pharmaceutical services (in community pharmacies), and access to and documentation of this information in PharmaNet (PharmaNet is a provincial database that houses almost every prescription that is dispensed in community pharmacies in BC, and is used by different care providers for different purposes).

FIPPA and PIPA outline the necessary provisions to protect and secure personal information against unauthorized use and disclosure, but data sharing permissions are complicated because the legislation is quite fragmented. Here are some examples of permissible information sharing:

- Under the Pharmaceutical Services Act and FIPPA, disclosure of personal information for market research purposes is not allowed, but it is acceptable for other research purposes as long as requests are submitted to a data stewardship committee.
- Under the Ministry of Health Act, the Minister of Health has the authority to collect, disclose or use personal information to or from any public body for what is referred to as 'stewardship purposes' – which is quite broad, including activities like planning, maintenance, and research.

New Federal Legislation to Report Adverse Drug Events

In 2014, a piece of legislation called Vanessa's Law (Bill C-17) was passed by the Government of Canada, introducing a series of amendments to the Food and Drugs Act. This legislation will require mandatory reporting of serious adverse drug reactions (a subset of adverse drug events) and medical device incidents from health care institutions to Health Canada. The regulations related to this portion of the legislation have yet to be defined, and we still don't know what kind of information requirements will be included. Based on what we know, in the absence of detailed regulations to support it, hospitals (and maybe other care providers) will be required to send patient specific information about adverse drug events to Health Canada. This would include information that links your identification to information about any serious adverse drug events you experience related to pharmaceuticals.

For more information on adverse drug reactions, our project, and relevant policy issues, please visit our website http://actionade.org/. Thank you again for participating!

Appendix B.

Focus Group Discussion Guide

I. Welcome

II. Introductions

III. Guidelines

- No right or wrong answers, just different points of view
- Session will be recorded; reminder of confidentiality
- Listen respectfully; only one person speaks at a time
- Ensure cell phones are on vibrate
- We will be asking you questions about adverse drug events—and in a minute we will define those for you. You are free to tell us about adverse drug events that you or someone you know has experienced, but you do not need to share that information with us.

IV. Introduce Topic

- Define ADEs: Adverse drug events are unintended and harmful events associated with medication use. They are a leading cause of emergency department visits and unplanned hospital admissions. Research has shown that 30 to 70% of ADEs are preventable due to repeat events and re-exposure to harmful drugs.
- 2-3 examples of ADEs

V. Questions

A) Questions about baseline perceptions

1. If you had a problem with a drug and your doctor knew about it, do you think that information is shared with other health care providers? Tell us what you think happens.

2. Is it the same for all providers? (e.g., your family doctor vs. the hospital vs. a specialist?)

3. Do you think there are differences in terms of type of information, in terms of what is and is not shared? Can you explain?

B) Experience with ADEs

1. Have you or someone you know ever experienced an adverse drug event?

1a. [*If yes*] Did you seek medical attention during or following this event? Where did you go? (e.g., family physician, emergency room, etc.)

1b. [*If yes*] Are you aware of whether your care provider documented that event at all? *Probe for further details.*

1c. Do you know if they reported that event to Health Canada's voluntary adverse drug reaction program? [*show reporting form]*

2. Health Canada's adverse drug reaction program has the option for patients to report their own reactions. Is self-reporting something that you would engage in if you were to experience an adverse drug event in the future?

2a. Why / Why not

2b. What do you think would make you more likely to self-report?

3. Thinking about reporting or documenting ADEs, who would you want to know about the event? Why?

4. Thinking about an ADE that either you or someone you know experienced, can you give any examples about how better information sharing might have led to a better end results?

C) Attitudes toward sharing medication information

1. Is there anyone you do not want to know about the medications you take? If so, who?

2. How comfortable are you with your care providers sharing your confidential medication information with each other?

2a. [*Based on responses, probe for details related to support for medication info sharing or opposition toward medication info sharing. What are the main drivers for support / opposition?]*

3. Is there specific information related to your medications you would like shared? Why?

4. Is there specific information related to your medications you would not want to be shared? Why?

5. Is there anything that would make you more comfortable with the sharing of this type of information? If so, what?

6. Are you comfortable having the provincial government determine what policies should be in place for sharing of medication information?

6a. If not, why not? What do you think they won't do well? What do they do well?

7. Is your opinion about policy setting around medication sharing the same or different for the federal government? Why or why not?

8. In British Columbia, five health authorities are responsible for the health delivery and planning in their respective geographic areas. Here at VGH, we are part of the Vancouver Coastal Health Authority. Are you comfortable having the health authorities determine the policies related to medication information sharing?

8a. If not, why not? What do you think they won't do well?

9. If you think that information should be shared, which methods would you prefer – on paper or electronically? Why?

10. Is there anything that could be done to make you more comfortable with sharing information electronically? If so, what?

11. Do you think you should be asked permission each time information about your medications is shared or used by care providers? (For example, when a doctor in the hospital faxes a discharge summary to your family doctor or pharmacist)

12. What about for research purposes? (For example, when you complete a survey about your health status)

13. What about information about you that would be used for care and research purposes? (For example, if you break your arm and arrive in hospital, and they record information about the incident explicitly for research purposes, and then that information is sent to a secure computer outside of the hospital)?

14. What about if the information collected for research purposes was information about pharmaceutical use?

15. Are there any other specific issues you are concerned about regarding sharing of patient information?

D) Attitudes toward data privacy

1. How secure do you think your confidential medical information is in health care facilities, like pharmacies, hospitals, and doctors' offices?

2. Do you think that removing specific, identifiable information about you will protect your data?

3. What laws in Canada are you aware of, if any, that protect your confidential medical information? [*Write down responses; fill in gaps as required, provide handout on privacy laws and Vanessa's law*]

4. Do you think there's a need for stronger legislation surrounding the protection of confidential medical information? What would that look like?

5. Given the information about different kinds of privacy legislation and the provisions in Vanessa's Law that require information about adverse drug events to be sent to Health Canada, how secure do you think your confidential medical information is with the government?

6. Do you think the laws governing privacy interfere with the provision of quality care?

7. From your perspective, what would be ideal in terms of allowing the sharing of information for health care?

8. Have you heard of any breaches of confidential medical data in the news recently?

8a. [If yes] – What did you hear?

8b. Did this change how you felt about sharing your data with care providers or the government?

8c. [If no] do you think hearing about these types of breaches would have an impact on your willingness to share your medical data with care providers or the government? Why or why not?

D) Concluding / wrap up question: How important do you think data sharing is in relation to data privacy? In other words, if privacy could not be guaranteed, would you still be willing to share medical data?

VI. Debrief

- Summarize responses to concluding statement
- Discuss current state of privacy of health information regulation
- Discuss Bill C-17
- Briefly explain our project
- Thank them for participating.

Appendix C.

Coding Structure

- Information sharing
    - Benefits
    - Patient role
    - Consent
        - Among health care providers for care
        - For research purposes
        - For care and research
        - For research about Rx use
    - Methods
        - All
        - Fax
        - Paper
        - Phone
        - Electronically
            - Ways to increase comfort
    - Preferences
        - Type of information would like shared
        - Type of information would not like shared
        - Who should know about medications taking
        - Who should not know about medications taking
        - Comfort with medication information sharing among health care providers
    - Perceptions / Experiences

        - In care contexts
            - Yes
            - No
            - Yes, I make sure of it
            - Unsure
            - Depends
        - Type of information shared / not shared
        - Informational discontinuity of care
    - Other issues
        - Access beyond health care providers
        - Length of retention
        - Current system is inefficient
- Adverse drug events
    - Experience with ADEs
        - Yes, me
        - Yes, someone I know
        - Description of the event
        - Sought medical attention
            - ED
            - GP
            - Specialist
            - No
        - Documentation of event
            - Yes
            - No
            - Unsure

        - Reporting of event (MedEffect)
            - No
            - Unsure
    - Self-reporting
        - Yes
            - Circumstantial
        - No
        - Unsure
        - Motivators
        - Questions, issues
    - MedEffect
        - Awareness of…
        - Perceptions toward…
        - Reporting preferences
    - Effect of information sharing on outcomes
        - Experienced benefit
        - Perceived benefit
        - No effect
    - Who should know about ADE
- Data privacy
    - Security of medical information in health care facilities
        - Baseline
        - If anonymized
    - Security of medical information with government
    - Awareness of breaches
        - Yes (+ description)

        - No
        - Effect of breaches on information sharing preferences
    - Willingness to share data if privacy not guaranteed
    - Who would want my data
    - Concern RE: data storage in US
- Privacy policy
    - Privacy legislation
        - Baseline awareness
        - Effect of legislation on provision of care
        - Perceived strength of legislation
    - Policy setting
        - Provincial government
        - Federal government
        - Health authorities
        - Other [unprompted]
- Balance information sharing and protection
- Recommendations for ADE documentation
- Stigma
- Trust

Appendix D.

Situational Mapping & Relational Analysis Maps

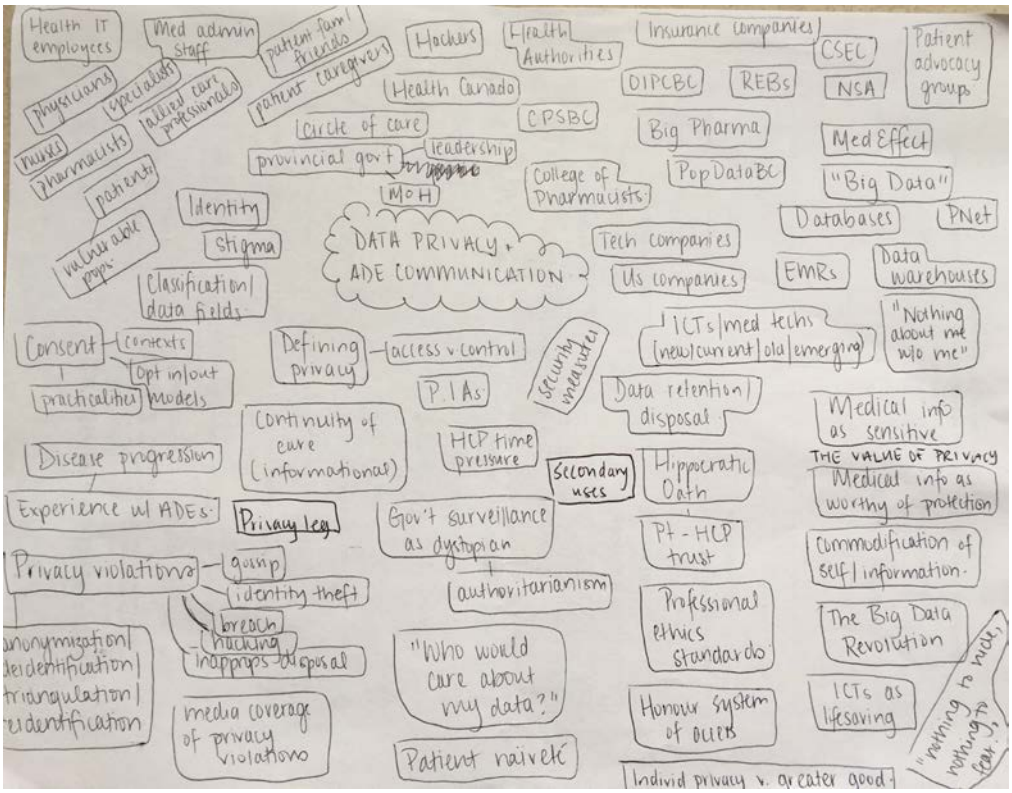

Figure D1. Messy Situational Map

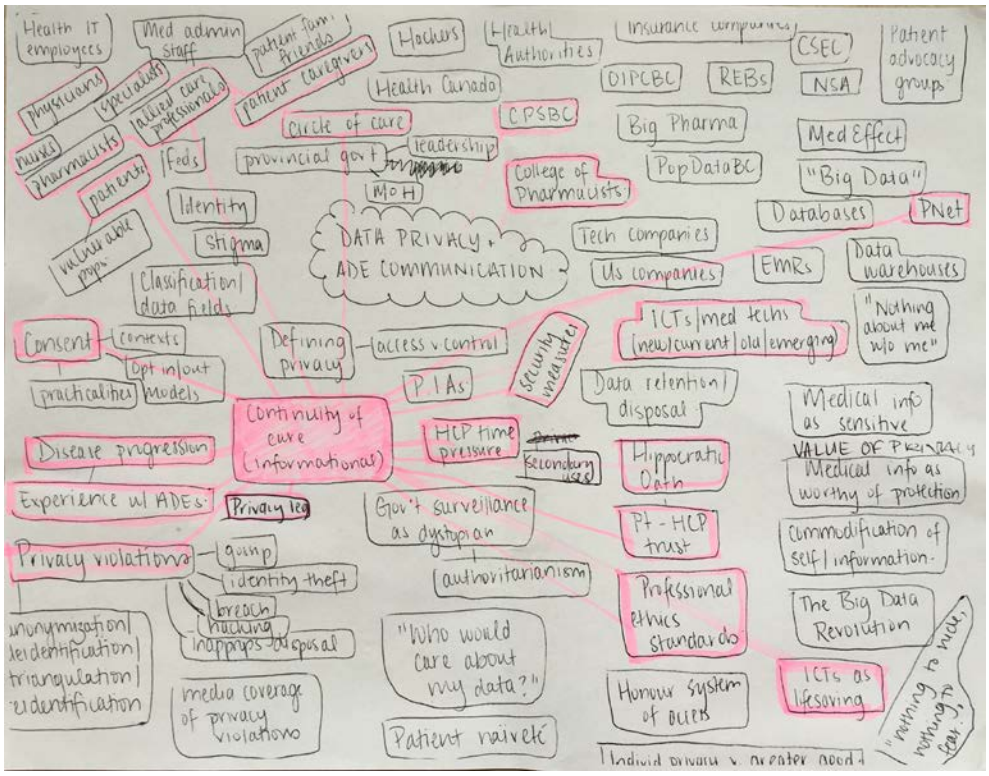

Figure D2. Relational Analysis: Informational Continuity of Care

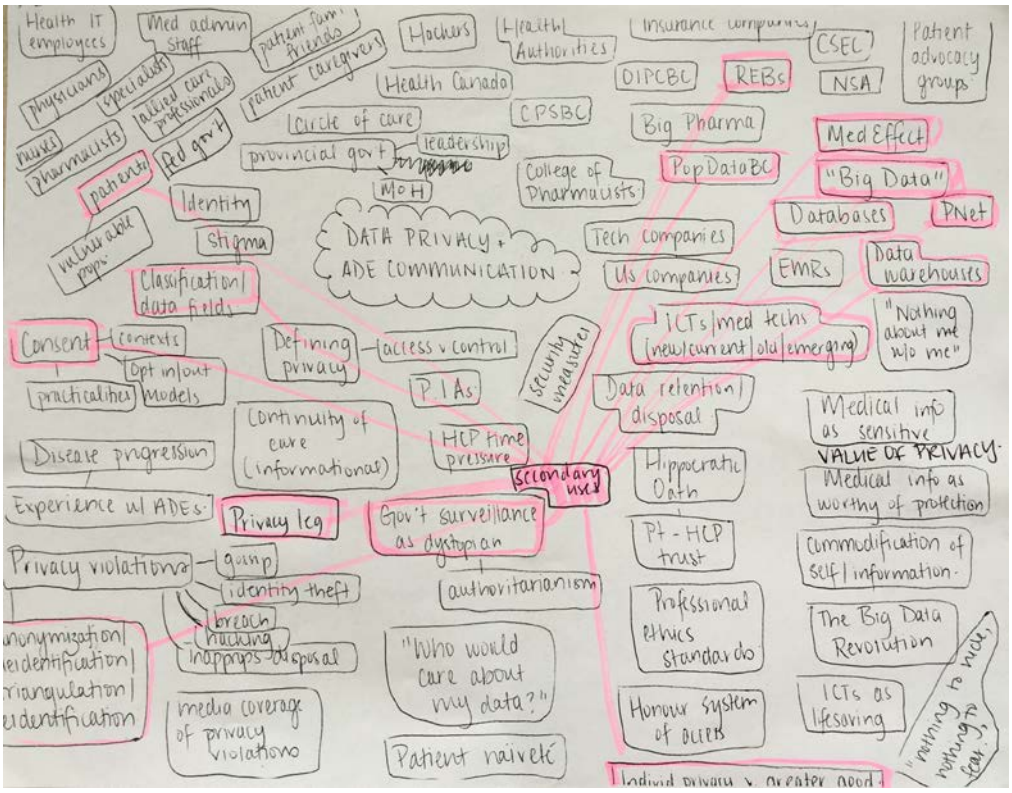

Figure D3. Relational Analysis: Secondary Uses

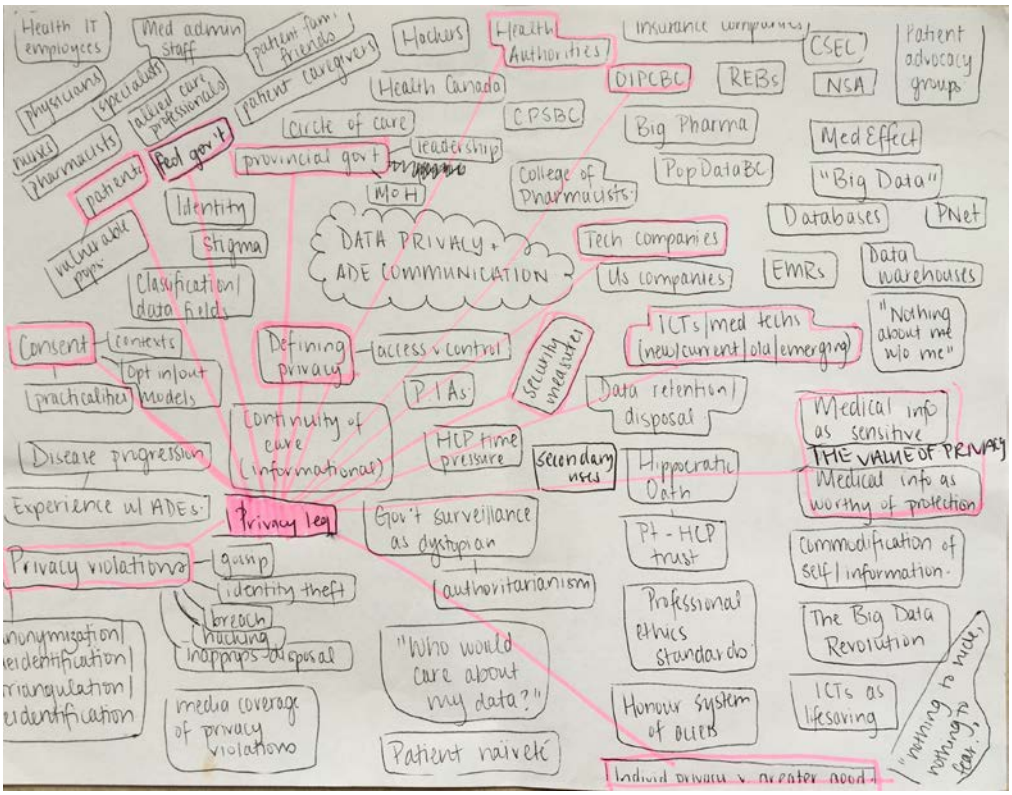

Figure D4. Relational Analysis: Privacy Violation

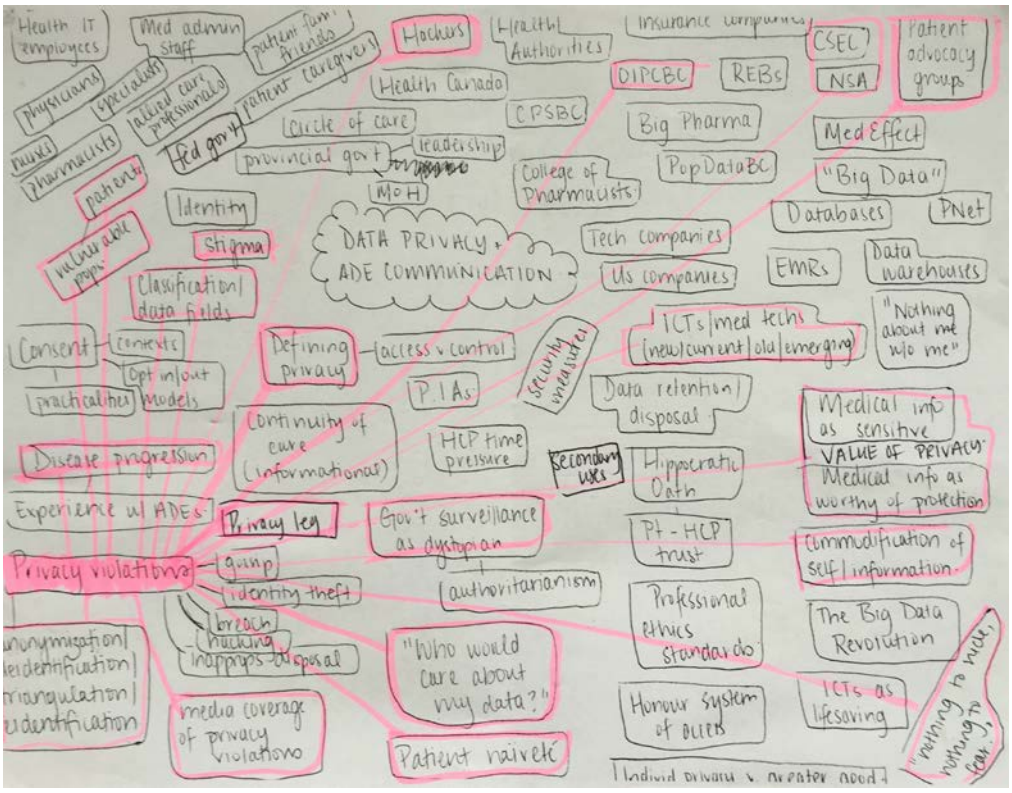

Figure D5. Relational Analysis: Privacy Legislation