A Framework for the Protection of Privacy in an Electronic Health Environment

by

Michelle Erin Gordon

A thesis submitted in conformity with the requirements for the degree of Master of Laws
Graduate Department of the Faculty of Law
University of Toronto

© Copyright by Michelle Erin Gordon (2010)
Abstract

This paper argues that given the proliferation of electronic health records (EHRs) in the health care system, legislative reform must occur to address the inadequacies of Ontario’s current health privacy legislation in accommodating EHRs. A coherent framework for legislation is necessary to capture the important role that privacy plays in public perception when it comes to legislating and managing EHRs in Ontario and, in turn, serve as a tool for legislators to understand the definitions and values of privacy associated with EHRs and the privacy problems worthy of protection in an electronic health environment. The failure to properly address these problems may lead to privacy losses and loss of public confidence in EHR systems. In applying this framework to three legislative options, it is evident that Ontario should amend the *Personal Health Information Protection Act, 2004* to better contemplate the privacy protections necessary in an electronic health environment.
Table of Contents

Chapter 1 Introduction ........................................................................................................... 1

Chapter 2 Background of Electronic Health Records .............................................................. 11

2.1 What are electronic health records? ....................................................................................... 11

2.2 The EHR landscape in Canada ............................................................................................ 14

2.2.1 Client, Provider, and Location Registries ................................................................. 15

2.2.2 Pharmaceutical Networks .............................................................................................. 16

2.2.3 Diagnostic imaging initiatives ....................................................................................... 16

2.2.4 Laboratory Information Systems .................................................................................... 17

2.2.5 Panorama/Health Surveillance ...................................................................................... 18

2.2.6 Telemedicine ................................................................................................................ 18

2.3 Funding EHRs in Canada ................................................................................................... 19

2.4 Importance of EHRs and privacy ......................................................................................... 23

2.4.1 Benefits of EHRs ........................................................................................................... 25

2.4.2 Privacy Concerns about EHRs .................................................................................... 26

2.4.3 Weighing the benefits and the harms ........................................................................... 29

Chapter 3 A Framework for Understanding Privacy in an Electronic Health Environment ...... 34

3.1 Definitions of Privacy in an Electronic Health Environment ................................................ 35

3.1.1 Privacy as control over personal information ............................................................ 36

3.1.2 Privacy as limited access .............................................................................................. 46

3.2 The Values of Privacy in an Electronic Health Environment: Personhood, Autonomy, and the Preservation of Dignity .................................................................................. 56

3.3 Privacy Problems in an Electronic Health Environment .................................................... 67

3.3.1 Control over personal information ............................................................................... 69

3.3.1.1 Surveillance ............................................................................................................. 69

3.3.1.2 Aggregation ............................................................................................................ 72
3.3.1.3 Secondary Use ........................................................................................................... 73
3.3.2 Limited Access .................................................................................................................. 74
  3.3.2.1 Identification .............................................................................................................. 75
  3.3.2.2 Breach of Confidentiality .......................................................................................... 76
  3.3.2.3 Disclosure ............................................................................................................... 79

Chapter 4 Options for Regulating the Electronic Health Environment in Ontario ............... 83

4.1 Option 1: Maintaining the Status Quo – The *Personal Health Information Protection Act, 2004* ......................................................................................................................... 85
  4.1.1 Background of *PHIPA* ................................................................................................. 86
  4.1.2 Application of Framework to Option #1 ..................................................................... 90
    4.1.2.1 Control over Personal Information ......................................................................... 90
    4.1.2.2 Limited Access ....................................................................................................... 96
    4.1.2.3 Privacy Problems ................................................................................................... 98

4.2 Option 2: Amend *PHIPA* by creating EHR regulations ........................................ 106
  4.2.1 Application of framework to Option #2 ................................................................... 109
    4.2.1.1 Control over Personal Information .................................................................... 109
    4.2.1.2 Limited Access .................................................................................................... 117
    4.2.1.3 Privacy Problems ................................................................................................. 120

4.3 Option #3: Create new provincial legislation specifically addressing EHRs .......... 127
  4.3.1 Background on Newfoundland’s *Personal Health Information Act* .................. 129
  4.3.2 Background on British Columbia’s *E-Health Act* ................................................. 130
  4.3.3 Application of Framework to Option #3 ................................................................. 133
    4.3.3.1 Control over Personal Information ..................................................................... 133
    4.3.3.2 Limited Access .................................................................................................... 137
    4.3.3.3 Privacy Problems ................................................................................................. 139

4.4 Determining the Best Legislative Route ........................................................................... 148
Chapter 5 Conclusion
Chapter 1
Introduction

When United States President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA), otherwise known as the economic stimulus bill, into law in February 2009, he announced to a joint session of Congress that the “recovery plan will invest in electronic health records and new technology that will reduce errors, bring down costs, ensure privacy and save lives”. The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the ARRA, promotes the adoption of health information technology by, among other things, imposing new privacy and security requirements by amending and expanding the Health Insurance Portability and Accountability Act (HIPAA). The privacy community paid close attention to the strong privacy provisions for the proposed medical health network, including audit trails, encryption, rights of access, breach notification requirements, and strong criminal and civil penalties for non-compliance. The Act allocated $19 billion of the $787 billion economic stimulus package to health information technology. This money will be used for, among other things, incentive payments over a five-year period for physicians and hospitals that use electronic health systems, with the ultimate goal of implementing an electronic health record (EHR) for every American by 2014. In the wake of economic downturn, electronic health records and the privacy protections necessary to implement these records were finally catching on in the public and government environment with the realization that EHRs are

necessary in order to improve the efficiency of the health care system and have the potential to
dramatically transform health records systems across the world.

The growing attention given to EHRs by the U.S. government and media undoubtedly has been seen in Canada as well. To date, the Canadian government has invested $2.1-billion to date in Canada Health Infoway, the non-profit federal organization established to promote and establish electronic health record systems. The provinces and health regions have, between them, committed about the same amount, bringing the total investment close to $4-billion. This includes $500-million announced in Prime Minister Stephen Harper's stimulus package in January 2009. In Canada’s Economic Action Plan, Budget 2009, the federal government claimed that its investment in Canada Health Infoway “will not only enhance the safety, quality and efficiency of the health care system, but will also result in a significant positive contribution to Canada’s economy, including the creation of thousands of sustainable, knowledge-based jobs throughout Canada.”

While comparisons between U.S. and Canadian laws and policies are worth noting, the expectations in Canada for the delivery of EHRs are undoubtedly and inherently different from those in the U.S. given the different nature of the health care systems. Since Canadians expect public health care delivery, they expect the delivery of electronic health records to be provided publicly as well, and with the same quality as the rest of the health care system. This means that the funding allocated in each respective country will not necessarily be proportional to the

---

4 André Picard “Building a coast-to-coast connection” The Globe and Mail (6 March 2009) [Picard].
6 Ibid.
population. This also means that the use of private electronic medical systems, such as Microsoft HealthVault and GoogleHealth, may be more widely accepted by Americans than Canadians, who tend to be more sceptical and less embracing of privatized health care delivery. However, it is relevant for Canada to look at the U.S. for guidance, especially given the proximity and similarities between the two countries, the likelihood for similar technologies to be used by both jurisdictions, the increased exchange of trans-border data flows involving personal health information, and the commitment in the U.S. to dedicate serious financial resources to creating and implementing electronic health records.  

The focus given to privacy with respect to EHRs in the U.S. recovery bill is long overdue. While privacy is not an unheard topic in the EHR landscape in Canada, sufficient attention has not been given to the importance of the implementation of privacy safeguards into EHRs in Canada. Privacy has become a popular and engaging topic and concern in Canadian society, but not necessarily in the context of EHRs. However, in light of the recent attention brought to EHRs during the eHealth Ontario scandal in the spring and summer of 2009, concerns around privacy have become more prominent and the discourse surrounding privacy protections and the EHR has become more public. For example, an editorial in the Windsor Star called for a legislative committee to “provide a much-needed forum to start looking at the privacy issues raised by the government's plan to load massive amounts of personal and sensitive health information online.” This article called for scrutiny of eHealth Ontario’s “ability to manage sensitive health information and ensure privacy”. Another article in the Ottawa Citizen

---

7 Picard, supra note 4.
9 Ibid.
championed the importance of personal control of health records in an electronic environment in light of three major privacy breaches.\textsuperscript{10} Still, in light of this public discourse, there is no real consensus on the definition of a privacy “right” or “problem”, and people often use the word “privacy” as a means to categorize or blame a wide variety of issues somehow associated with privacy.

The Supreme Court of Canada has stated that the “protection of privacy is a fundamental value in modern, democratic states”\textsuperscript{11}, is worthy of constitutional protection, and also has “profound significance for the public order”.\textsuperscript{12} A review of scholarly literature on privacy is consistent with the patchwork approach to privacy by Canadian courts. In Canada, some of the debate remains focused on whether we have, indeed, a right to privacy at all in situations not involving the criminal law.\textsuperscript{13} There does not seem to be a consensus over whether privacy is a public or a private right. This lack of consensus may contribute to the fact that strong, coherent privacy protections specifically addressing electronic health records have not yet been built into existing Canadian health privacy legislation in a consistent manner.

Health information is arguably the most intimate, personal, and sensitive of any information maintained about an individual. A consensus on the definition and value of health privacy needs to be achieved, given the concern Canadians place on their right to health privacy. As health records start being maintained in electronic form containing comprehensive data on individuals accumulated over time, the development of the electronic health record (EHR)

\begin{flushend}
\textsuperscript{10}“Give people control over online health records,” Editorial, \textit{The Ottawa Citizen} (12 June 2009).
\textsuperscript{11} \textit{Dagg v. Canada (Minister of Finance)}, [1997] 2 S.C.R. 403 at para. 65, La Forest J., dissenting [\textit{Dagg}].
\textsuperscript{13} Richard B. Bruyer, “Privacy: A Review and Critique of the Literature” (2006) 43 Alta. L. Rev. 553 at 554 [\textit{Bruyer}].
presents a great challenge to the right to privacy in Canada. Once Canadians’ health records are electronically entered and maintained, their potential for various uses, such as health research, public health and law enforcement, make them a valuable asset for some uses but also a potential threat to individual control, autonomy, and liberty. Further, these databases have the potential to be merged with other electronic sources, thereby dramatically increasing both their value and their threat.

Since personal health information will soon be able to be accessed entirely in electronic form, comprehensive regulatory oversight is required in order to ensure that Canadians’ privacy rights are properly protected. Control mechanisms must be implemented so that personal health information is properly accessed by users for proper purposes and with the patient’s consent. There must be greater recognition that creating electronic health records that will improve healthcare delivery will likely require not only a financial commitment by the government, but also the support of health care providers and patients alike. In order to gain and maintain this support, proper controls must be built into electronic health records and into the supporting legislation to ensure that patients’ sensitive personal health information will not be compromised in the electronic environment and that their privacy will be assured.14 This sentiment was recently echoed by Senator Patrick Leahy of the United States Senate when he stated: “Without adequate safeguards to protect health privacy, many Americans will simply not seek the medical

---

treatment that they need for fear that their sensitive health information will be disclosed without their consent.”

Canada Health Infoway identifies privacy and consent legislation as a key enabler of its ultimate vision for health information technology in Canada. In its 1999 report, the Advisory Council on Health Info-Structure delivered a similar message that harmonizing legislative rules for the use of personal health information for health care purposes is essential for realizing the vision of a Canadian health info-structure. The Canadian Medical Association recognized the difficulty of this task as follows: “Many laws, practices and initiatives may not withstand the kind of scrutiny deemed necessary and reasonable for the protection of privacy and the trust and integrity of the therapeutic relationship.”

In this paper, I will argue that given the accelerated development of EHR systems in Canada and the increased interest of Canadians in managing their personal health information, particularly in an electronic environment, legislators must make quick progress in ensuring that a proper legal framework is in place to regulate EHRs. In particular, I will focus on how legislation in Ontario must progress in order to address the proliferation of EHRs in Canada’s most populous province and the current weaknesses of Ontario’s health privacy legislation, the

---


In making this argument, I will establish a framework for privacy in an electronic health environment.

In Chapter 2, I will provide general background on the definition and meaning of electronic health records and on the current electronic health landscape in Canada in order to inform the discussion in this paper. I will also provide a broad overview of the importance of privacy in an electronic health environment and assess some common benefits and drawbacks associated with EHRs in Canada.

In Chapter 3, I will set out a framework that sets out to capture the important role that privacy plays in public perception when it comes to legislating and managing the provincial EHR in Ontario. In determining this framework, I contend that in order to determine the best legislative options for privacy in an electronic health environment, we must understand privacy in three different ways – as a definition, as a value, and as a useful concept for determining privacy problems worthy of legal protection. Regulators, politicians, and policymakers need to understand the definitions and values of privacy associated with electronic health systems and the privacy losses that may result when these definitions and values of privacy are not properly addressed.

In developing this framework, I will look at existing theories and conceptions of privacy and judicial decisions. I will establish this framework by looking at two traditional definitions of privacy that are relevant in an electronic health environment, namely control over personal information and limited access. I will then examine the values that these definitions of privacy protect in the electronic health environment by focusing on how autonomy, dignity, and
personhood are values of privacy that are necessary to protect in this context. Finally, I will use these definitions as the basis by which to examine privacy as a useful concept in the legal context in order to identify which privacy problems and losses deserve legal protection in an electronic health environment.

In determining and assessing these privacy problems, I will adopt parts of a recent theory of privacy put forward by Daniel Solove, an American privacy academic and law professor at the George Washington University Law School. In his recent book, *Understanding Privacy*, Solove contends that since new technologies have generated a panoply of different privacy problems, a new taxonomy is therefore needed to address privacy violations for contemporary times. The purpose of his taxonomy is to “provide a more pluralistic understanding of privacy”. Of specific interest to the emerging technology of electronic health records, Solove writes: “The way we conceptualize privacy is of paramount importance for the information age because we are beset with a number of complex privacy problems that cause great disruption to numerous important activities of high social value.” As Solove suggests, in developing this privacy framework, I will focus on the importance of conceptualizing privacy in the modern electronic health environment in order to understand the myriad of privacy problems associated with implementing a provincial and federal EHR system. Just as Solove aims to aid the crafting of law and policy with his taxonomy, I hope to provide a useful framework for the future development of health privacy legislation and to encourage informed discussion about possible

regulatory choices while electronic health records are still in the development stages and existing health privacy legislation is still under review.

In Chapter 4, I will set out and explore three practical, but non-exhaustive, options that may be suitable for addressing the regulation of EHRs in Ontario, and apply this new framework to these options in order to determine the best approach for regulation. First, I will look at whether maintaining the status quo by keeping PHIPA in its current form is a viable option. Second, I will explore the option of amending PHIPA through EHR-specific regulations by examining how other Canadian provinces have updated their health privacy legislation to accommodate EHRs. Third, I will examine the option of enacting separate, EHR-specific legislation in Ontario, as was recently done in British Columbia. In exploring these options, I will address the challenges involved in developing health privacy legislation that properly encompasses modern electronic health records. In applying this new framework to the three possible options for regulation, I will demonstrate how the different definitions of privacy and various current approaches to the regulation of electronic health records in Canada must be considered in order to determine the best approach for Ontario to take with respect to ensuring that its citizens’ privacy rights are best protected as the province’s health records shift to electronic form.

Finally, in Chapter 5, I will conclude the analysis by summarizing the application of the framework set out in Chapter 3 and make recommendations for proceeding with the regulation of EHRs in Ontario. Although there are countless of other issues that arise in the context of privacy in an electronic health environment, this paper will not serve to address interrelated questions, such as those surrounding federalism, harmonization of health privacy legislation across provinces, or comparisons to EHR progress in other countries. Further, where this paper
recommends the need for changes to legislation, it does not attempt to recommend specific draft language for any potentially new or amended legislation.
Chapter 2
Background of Electronic Health Records

Prior to developing a framework for privacy in the context of electronic health records (EHRs), it is first important to understand the meaning of an electronic health record, both generally and in the Canadian context. To this end, this chapter will first look at the definition and meaning of the electronic health record in order to establish the scope of discussion for this paper. Second, this chapter will survey the EHR landscape in Canada and in Ontario, and provide examples of some common EHR-based projects being developed in various provinces across the country. Third, I will assess the reasons why privacy is important in an electronic health environment and weigh the benefits and harms associated with this new technology. Finally, this chapter will look at Canadians’ views on EHRs by reviewing recent surveys and opinions in order to understand why Canadians are concerned with EHRs as a particular privacy problem worth being addressed by regulators and policymakers.

2.1 What are electronic health records?

It is generally recognized that EHRs are an important emerging technology that offers the potential to dramatically transform the health care system. In February 1999, the Advisory Council on Health Info-Structure, commissioned by the federal Minister of Health, released its final report that articulated a vision for a pan-Canadian health info-structure. The Council referred to the importance of EHRs as follows:

Patient-based health records are fundamental to provincial and territorial health info-structures. However, they have the potential for serious violations of privacy. The Council believes that, with particular care, electronic health records can actually enhance privacy protection, improve patient care, enable telehealth, empower citizens
through greater control of their own health records and serve as the foundation for an ever-improving information and evidence-based health system.\textsuperscript{22}

In 2002, the Romanow Commission’s report – \textit{Building on Values: The Future of Health Care in Canada} – found that paper records are increasingly becoming obsolete and inadequate and that EHRs are “one of the keys to modernizing Canada’s health care system and improving access and outcomes for Canadians”.\textsuperscript{23}

According to Canada Health Infoway, the EHR is a “secure, digital record of your medical history, stored and shared via a network of EHR systems”\textsuperscript{24} and a “secure and private lifetime record of an individual’s health and care history, available electronically to authorized health care providers”.\textsuperscript{25}

This paper will focus on the above definition of the EHR, and may sometimes refer to “EHRs”, depending on the context. It is important to understand the difference between the EHR and other types of medical records, as the terminology is often used interchangeably and often inaccurately. An Electronic Medical Record (EMR) is a provider or site-specific record of the interactions with a specific patient. An EMR is a subset of the EHR and is maintained by providers, such as physicians or hospitals, in order to meet their fiduciary duties to their patients, as well as the requirements of their regulatory bodies. In other words, is it similar to the typical paper-based chart found in doctors’ offices, but is kept in electronic format that is created by

\textsuperscript{22} Advisory Council on Health Infostructure, “Paths to Better Health”, \textit{supra} note 17 at 48.


\textsuperscript{25} Canada Health Infoway, “A look at the future” (2008), online: Canada Health Infoway <http://www.infoway-inforoute.ca>. 
clinicians and is only accessible to other clinicians. The most common example of an EMR would be one maintained by an independent hospital or organization, such as the Ontario Patient Results Online application, which allows authorized clinicians to view patient results through a common, secure, and seamless user interface across several teaching hospitals and clinics associated with the University of Toronto. Another example was seen in the ‘medical passport’ system used by the Vancouver Organizing Committee for the 2010 Olympics as a means to transport the athletes’ medical history in electronic form.

A Personal Health Record (PHR), on the other hand, focuses on patient control and may or may not be connected to an EHR or other clinical systems. A PHR is a web-based application that allows patients to initiate, maintain and self-record information about themselves and to access their test results without their doctor. An ideal PHR would provide a complete and accurate summary of the health and medical history of an individual by gathering data from many sources and making this information accessible online to anyone who has the necessary electronic credentials to view the information. PHRs have been making news headlines in the past year, with large organizations introducing new PHR platforms, such as Google announcing a PHR pilot with the Cleveland Clinic called “Google Health”. This project enables users to voluntarily sign up for an account, which they can then log into at partnered health services providers and also merge potentially separate health records into one centralized Google Health profile. In Ontario, Sunnybrook Hospital has created MyChart™, an online website where patients can create and manage their personal health information based on clinical and personal

26 For more information see, for example: Matthew Anderson “Moving eHealth up the Agenda” (17 June 2005), online: Canadian Healthcare Network <http://www.chmonline.ca/eHealth2005/PDFs/Matt%20Anderson.pdf>.
Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, is a vocal proponent of MyChart™, which she carries on a memory stick.29

2.2 The EHR landscape in Canada

In Canada, the provinces have been tasked with the challenge of implementing electronic health systems for their respective jurisdictions, leading to diverse solutions that reflect the unique nature of each province. Despite these differences, the provinces have each taken similar approaches to developing a provincial EHR that includes several building blocks – such as client registries, drug information networks, and image sharing networks – that will eventually integrate into a pan-Canadian EHR. Of the Canadian provinces, Alberta has led the way with respect to a pan-provincial EHR with the development of “Netcare”.

Canada Health Infoway is tasked with ensuring that the provinces and territories, health care providers and technology solution providers collaborate to accelerate the use of EHRs in Canada. Infoway seeks to establish a baseline EHR for all Canadians by 2015.30 As of September 30, 2009, Infoway had approved funding for 291 projects across Canada, and planning had been completed for 173 of these projects.31 Of these projects, 30 have been approved for Ontario, more than any other province.32 Some examples of the common EHR-based projects being developed in various provinces are included in the discussion below in

---

28 See Sunnybrook Health Sciences Centre, “Patient Care: MyChart”, online: Sunnybrook Health Sciences Centre <http://www.sunnybrook.ca/content/?page=mychartlogin_learnmore>.
order to provide an understanding of where these projects are heading and of the complex environment that legislators must face.

2.2.1 Client, Provider, and Location Registries

Several provinces have developed or will develop a common set of registries that allow for the secure and unique identification of clients, providers, and service locations. For example, in Alberta, the patient/client registry allows Alberta’s Netcare to function by identifying each patient uniquely as the first step to securely adding health information to their record. The provider registry supports the secure authorization and authentication of all authorized health service providers accessing Alberta’s Netcare. In Saskatchewan, the Provider Registry System stores and manages data about health care providers by uniquely identifying providers with a Common Provider Number, while the Shared Client Index/Client Registry automatically matches patient identifiers and demographics from various provincial and regional health sources in order to create a single “source of truth” for individual access to the health system. Newfoundland and Labrador’s Client Registry is a tool currently operating in that province that holds demographic and administrative information related to individuals who receive health and community services in that province. Without these registries to provide accurate, up-to-date information about individuals, the EHR will not function properly.

---

2.2.2 Pharmaceutical Networks

Most provinces include in their e-health strategy some type of pharmaceutical or drug network, especially given the increased benefits that a centralized drug prescribing and record-keeping system bring to improve health care. These networks provide health providers with prescription information from physicians, prescribed dispensing information from pharmacies, drug-to-drug interaction alerts to avoid prescription conflicts, and a database of available drugs and their common dosages. The benefits include ensuring that only authorized health providers are able to view drug information and eliminating fraud by patients seeking to overdose or forge physician signatures.

For example, in Alberta, all pharmacists working in the province’s community-based pharmacies are required to submit drug dispensing information to the Ministry to be entered into the Pharmaceutical Information Network.36 In British Columbia, PharmaNet records information on all prescriptions dispensed in community pharmacies in the province.37

2.2.3 Diagnostic imaging initiatives

These projects allow diagnostic reports and images, such as CT scans and MRIs, to be made available to health care providers on a provincial, and eventually federal, level. As of July 2009, all of Ontario’s 148 hospitals were able to produce and share filmless diagnostic images including x-rays, CT scans and MRIs within their facilities using picture archiving and

communications (PACS) technology.\textsuperscript{38} The Alberta Netcare EHR currently contains 90\% of the diagnostic reports and images produced in province.\textsuperscript{39} In British Columbia, the Connecting Diagnostic Imaging (CDI) project provides health care providers with access to digital diagnostic images via the B.C. EHR regardless of where the patient received care.\textsuperscript{40} In Saskatchewan, the RIS/PACS initiative enables a common shared Radiology Information System (RIS) and PACS infrastructure for the province.\textsuperscript{41} In August 2008, Newfoundland’s PACS was deployed in regional health authorities and become interoperable with the province’s Client Registry.\textsuperscript{42}

2.2.4 Laboratory Information Systems

These systems serve to provide consolidated diagnostic laboratory test results to health care providers across a province and, eventually, across the country. The electronic transfer of this information enhances clinical workflows and the quality and utilization of laboratory services, such as blood tests. In Ontario, the Ontario Laboratory Information System connects the 40,000 authorized healthcare providers who order laboratory tests and use their results, as well as the 650 community, hospital and public laboratories and specimen collection centres that

\textsuperscript{38} eHealth Ontario, Press Release, “All Ontario hospitals now filmless; another step towards comprehensive ehealth system achieved” (15 July 2009), online: eHealth Ontario <http://www.ehealthontario.on.ca/News/filmless.asp>.


\textsuperscript{40} British Columbia Ministry of Health Services, “Connecting Diagnostic Imaging”, online: Government of British Columbia <http://www.health.gov.bc.ca/ehealth/cdi.html>.


\textsuperscript{42} Newfoundland and Labrador Centre for Health Information, “Electronic Health Record Fast Facts” (October 2008), online: Newfoundland and Labrador Centre for Health Information <http://www.nlchi.nf.ca/pdf/EHR_FF_October_2008_FINAL_4_pager.pdf>. 
perform tests.\textsuperscript{43} In B.C., this project is known as the Provincial Laboratory Information System,\textsuperscript{44} and in Saskatchewan it is the Saskatchewan iEHR/Lab Results Repository.\textsuperscript{45}

2.2.5 Panorama/Health Surveillance

Panorama is the Pan-Canadian health surveillance software application being run and piloted under the Public Health Information Program in British Columbia, with plans to implement across Canada. The application will help facilitate the management of communicable diseases, outbreaks, immunizations, and vaccine inventory while helping improve public health information management.\textsuperscript{46}

2.2.6 Telemedicine

Telemedicine refers to the delivery of health-related services and information using telecommunications technologies. In Ontario, the Ontario Telemedicine Network uses two-way videoconferencing systems and diagnostic instruments like digital stethoscopes, otoscopes and patient examination cameras to help health care providers deliver clinical care and professional education to their patients, regardless of location in the province.\textsuperscript{47} In British Columbia, the

\begin{itemize}
\item\textsuperscript{43} eHealth Ontario, “Laboratories”, online: eHealth Ontario \(<\text{http://www.ehealthontario.on.ca/clients/labs.asp}>.\)
\item\textsuperscript{44} British Columbia Ministry of Health Services, \textit{Project Summary: Provincial Laboratory Information System (PLIS) and Interoperable Electronic Health Record (iEHR)} (August 2007), online: Government of British Columbia \(<\text{http://www.health.gov.bc.ca/ehealth/pdf/PLIS_project_summary.pdf}>.\)
\item\textsuperscript{45} Government of Saskatchewan, “iEHR/Lab Results Repository”, online: Government of Saskatchewan \(<\text{http://www.health.gov.sk.ca/ehr}>.\)
\item\textsuperscript{46} British Columbia Ministry of Health Services, “Public Health Information Project”, online: Government of British Columbia \(<\text{http://www.health.gov.bc.ca/ehealth/phip.html}>.\)
\item\textsuperscript{47} Ontario Telemedicine Network, “Who we are”, online: Ontario Telemedicine Network \(<\text{http://www.otn.ca/en/otn/who-we-are}>.\)
\end{itemize}
Telehealth Office is run by the Ministry of Health Services, and in Saskatchewan, Telehealth Saskatchewan is a Saskatchewan Health program.

### 2.3 Funding EHRs in Canada

As of March 2009, the federal government had invested $2.1-billion in Canada Health Infoway, including $500-million announced in Stephen Harper's recent stimulus package. In March 2009, the Ontario government unveiled a $2.1 billion strategy for eHealth Ontario, the new provincial agency that promises to give every diabetic patient in the province an electronic health record by 2012, every patient an electronic health record by 2015, and to connect doctors, patients and pharmacists electronically to better manage the flow, safety and effectiveness of prescription drugs and cut wait times at Ontario hospitals. The provinces and health regions have, between them, committed about the same amount, bringing the total investment close to $4-billion.

Despite all this funding, Ontario continues to lag behind other jurisdictions with respect to progress for EHRs. As of March 2009, Canada Health Infoway reported that only about 17 per cent of Canadians had a core electronic health record. Infoway had initially aimed to help 50 per cent of Canadians obtain a core EHR by 2009, and now aims for 50 percent by the end of 2010 and 100 percent by 2016. Only 25 percent of Ontario family doctors have electronic

---


50 Picard, supra note 4.


records compared with 50 percent in Alberta.\textsuperscript{53} This is a low rate compared to other jurisdictions, including the Netherlands which has a 98 percent electronic rate, New Zealand with 92 per cent, the U.K. with 89 percent, and Australia with 79 percent. The U.S. currently fares worse than Canada, but this may change with President Obama’s promises to digitize medical records as part of the stimulus package.\textsuperscript{54}

There are several reasons for this slower pace of development in Ontario. First, Ontario has lagged behind because of the enormous expense associated with implementing electronic health records. As Canada’s most populous province, Ontario needs the proper funding to support EHR development. Canada Health Infoway estimates that an integrated health record for Canada would have estimated capital expenditures of $10 billion. However, putting this figure into perspective, Canada’s health system spends that every three weeks.\textsuperscript{55} Infoway claims that EHRs will ultimately save the healthcare system $6 to $7 billion a year but will require a one-time investment of $350 per Canadian; however, the federal government has so far only contributed about $50 per person\textsuperscript{56}, which is not sufficient for Canada’s largest and most populous province.

Second, given the massive expense and political pressure behind the implementation of EHRs, the provincial agency tasked with implementing the EHR in Canada’s largest province by 2015 has been plagued with controversy, both when it was called Smart Systems for Health

\textsuperscript{53} Michael Rachlis “Losing track of big picture at eHealth” \textit{The Toronto Star} (12 June 2009), online: The Toronto Star <http://www.thestar.com/comment/article/649474> [Rachlis].


\textsuperscript{55} Rachlis, supra note 53.

\textsuperscript{56} Hadzipetros, supra note 54.
Agency (SSHA) and later when it was renamed eHealth Ontario.\textsuperscript{57} In May 2009, EHRs were given unwanted media attention when eHealth Ontario was at the centre of a politically-charged media scandal surrounding its spending.\textsuperscript{58} Prior to that, SSHA had started creating a “secure, integrated, province-wide information infrastructure” in 2003, but was criticized three years later when it had made little progress in its strategic direction while spending questionable amounts of money. In a review by a consulting firm in late 2006, SSHA was found to be not well-regarded in the health care community and to have “incomplete and not widely understood privacy policies.”\textsuperscript{59} In 2007, Ontario’s Information and Privacy Commissioner conducted a review of the SSHA and harshly criticized it for privacy and security issues. SSHA never recovered from these critiques, and in late 2008, Ontario Premier Dalton McGuinty decided to shut down SSHA and start over with the new eHealth Ontario. In May 2009, eHealth Ontario came under political and media fire over allegations of improperly tendered contracts to consultants. The Ontario Auditor General Jim McCarter began examining the finances of eHealth Ontario and SSHA since fall 2008, and released his review in October 2009. The report focused on the overall progress of the EHR initiative given the $1 billion in EHR expenditures made in the prior seven years. The Auditor General also found that consulting contracts were sole-sourced to consultants by the Chief Executive Officer of eHealth Ontario and that questionable procurement practices


\textsuperscript{58} See e.g. Theresa Boyle “Province struggles to digitize health records” (20 June 2009), online: The Toronto Star \texttt{<http://www.thestar.com/news/ontario/article/654002>}.

took place at the agency and its predecessor agencies. Given the intense media scrutiny and government audits, eHealth Ontario has fallen behind and this lack of progress will undoubtedly impact its short and long-term goals.

Third, despite the socialized nature of the Canadian health care system, the funding is the most socialized part while other key parts are private. This funding problem is evident across Canada, and may be demonstrated through the lack of funding in Ontario. Most of Ontario’s 20,000 doctors are in private practice and the 140-plus hospitals are generally private, non-profit corporations with independent boards and some private funding. While over a dozen electronic systems are approved for doctors’ offices in Ontario, these offices cannot all communicate with each other and with the hospitals because the Ontario government has not contributed sufficient funds. According to one eHealth Ontario executive, Ontario must encourage a greater number of physicians to utilize EHRs; while the government absorbs 70% of the costs associated with a physician’s move to EHRs, only about 40% of Ontario physicians receive this funding. Despite all the complaints about misspending on EHRs in Ontario, the government still needs to contribute the money to ensure that money is spent effectively and efficiently so that the many existing and developing electronic health systems in Ontario can become interoperative.


61 Rachlis, supra note 55.

2.4 Importance of EHRs and privacy

The development of electronic health records (EHRs) is arguably the greatest challenge facing our notions of health information privacy today. Some argue that it is currently the biggest issue in the Canadian health care system. For example, in a 2008 Globe and Mail article, Dr. Michael Evans wrote: “When we think of holy grails in medicine, we tend to think of cures for cancer and miraculous surgical recoveries. But for many experts in the Canadian health-care system, the biggest grail is a universal EHR.”\(^{63}\) When the Advisory Council on Health Info-Structure released its final report, it stated that it believed that “with particular care, electronic health records can actually enhance privacy protection, improve patient care, enable telehealth, empower citizens through greater control of their own health records and serve as the foundation for an ever-improving information and evidence-based health system.”\(^{64}\)

The challenge underlying the intersection of privacy, electronic health records, and legislation is that these records contain information about individuals that is inherently private. Once EHRs are implemented across the country according to Canada Health Infoway’s vision, Canadians’ personal health information will be collected, used, and disclosed in a way that on one hand is unfathomable and on the other hand is entirely beneficial. EHRs will include highly personal information, such as mental health history, genetic dispositions, and sexual diseases, which could be potentially embarrassing or damaging if placed in the wrong user’s hands. However, EHRs will also include information that may facilitate life-changing medical care,


\(^{64}\) Advisory Council on Health Infostructure, “Paths to Better Health”, *supra* note 17 at 3-10.
such as the use of diagnostic images across borders and access to prescription drug information that may prevent replication and abuse.

Recognizing the challenges involved in addressing privacy issues while developing a pan-Canadian EHR, the Romanow Commission on the Future of Health Care in Canada recommended that “Canada Health Infoway should...be responsible for developing a pan-Canadian electronic health record framework built upon provincial systems, including ensure the interoperability of current electronic health information systems and addressing issues such as security standards and harmonizing privacy policies.”65 In October 2002, the Senate Kirby Report on Health Care stated the following about the importance of EHRs:

An important characteristic of an EHR system is that it can make patient data available to health care providers and institutions anywhere on a need-to-know basis by connecting interoperable databases that have adopted the required data and technical standards. Not only can an EHR system greatly improve quality and timeliness in health care delivery, it can also enhance health care system management, efficiency and accountability. Moreover, the data collected from an EHR system can provide very useful information for the purpose of health research.66

Specifically on the topic of privacy and the EHR, the Report noted that “[t]he issue of privacy, confidentiality and protection of personal health information in the context of an EHR system is perhaps the most sensitive one raised during the Committee’s hearings on this question.”67

By recommending the national implementation of EHRs, the Romanow and Kirby reports provided significant media attention to EHRS, as well as attention to policymakers. Both reports

65 Romanow Report, supra note 23 at 249.
67 Ibid.
recognize the potential of EHRs to improve health care delivery and enhance health system reform, and are also sensitive to both the increased benefits and growing concerns surrounding the privacy of personal health information.

2.4.1 Benefits of EHRs

Academic and technical literature suggests that EHR implementation could greatly improve health care delivery to individual patients by helping health care providers share accurate patient health information quickly and across different health care systems.\(^{68}\) The Romanow Report found that there are ―clear benefits to Canadians from electronic health records‖, including giving them ―ready access not only to their own personal health care information but also to a wealth of trusted, credible information on a variety of health topics.‖\(^{69}\)

Lawrence Gostin argues that the ―ability of the health care system to function effectively depends in part on the accuracy, currency, completeness and availability of health data.‖\(^{70}\) EHRs have the potential to improve doctor-patient communication, advance health care research, facilitate patient access to prescription renewals and cut health care costs by evaluating areas requiring improvement.\(^{71}\) Research suggests that access to comprehensive EHRs reduces health care costs by, among other things, allowing health care providers to respond to patient inquiries by other means.\(^{72}\)


\(^{69}\) Romanow Report, supra note 23 at 80.


\(^{72}\) Amanda Cornwall, “Connecting Health: A Review of Electronic Health Record Projects in Australia, Europe and Canada” Public Interest Advocacy Centre (November 2002) 2 [Cornwall, “Connecting Health”].
The widespread implementation of EHRs is also known to benefit health research and program evaluation, including monitoring population health patterns, identifying at-risk populations, determining the effectiveness of treatment, and assessing the adequacy and appropriateness of care. In Canada, cancer organizations and health services research institutes have used electronic cancer registries and other electronic research tools to provide essential information about Canadians’ health status.\textsuperscript{73}

### 2.4.2 Privacy Concerns about EHRs

The major concern behind EHRs is that the increased flow of information leads to further risks about privacy and confidentiality, especially given increased vulnerability in electronic security and human judgment. One of the greatest privacy concerns with EHRs stems from the fundamentally different way in which information is gathered in an electronic society. Lawrence Gostin notes that in this modern era, the traditional rule of confidentiality in the physician-patient relationship does not work in the same way as it does in a paper-based system. While patient records used to be gathered by a single primary care physician, health records today contain a substantial amount of information gather from both primary and secondary sources, including specialists, laboratories, researchers, and insurers. Health records are no longer maintained only by the primary care physician, but also by government agencies, health database organizations, and information brokers and are ultimately collected and transmitted electronically and linked to other data.\textsuperscript{74} This means that patients fear losing control of their personal health information and are uncertain of who will be able to access this private information.


\textsuperscript{74} Gostin, \textit{supra} note 70 at 512.
There is also a fear of the “function creep” phenomenon, which suggests that uses of EHRs will expand to encompass activities not originally foreseen, such as data matching between EHRs and personal information databases unrelated to health care. Further, the nature of electronic information means that the improper disclosure of confidential health information can have further-reaching harmful consequences for patients than a breach involving paper records.

In British Columbia, which has begun launching its eHealth systems ahead of Ontario, organizations concerned about medical privacy have started a campaign called “B.C.’s Big Opt-Out”. This campaign stresses the right of those living in B.C. to determine for themselves whether or not to participate in the provincial EHR by providing or withholding informed consent, as opposed to the proposed implied consent model. The campaign organizers are particularly concerned that personal health information made available to the provincial EHR for primary purposes, such as doctors directly caring for their patients, will be made readily accessible to third parties, such as government bureaucrats, technicians, and the Health Minister for secondary purposes not directly related to the provision of health care for patients. There is a concern that the information being stored in these large health information databanks will not be properly de-identified and that proper attention to secondary uses of this data has not been given by decision makers.

In an article written during the aftermath of the eHealth Ontario scandal in June 2009, one commentator noted that “[p]rivacy issues, not untendered contracts should be the greatest

75 Ries, “Patient Privacy”, supra note 71 at para. 11.
worry for Ontarians when it comes to eHealth." He pointed to three potential privacy concerns associated with storing health records online. First, since thousands of health care professionals will have access to the electronic health system, there is a high risk of privacy breaches. In order to reduce the number and frequency of breaches, eHealth Ontario would need to act preventively as opposed to reactively. Second, as with other online systems, the EHR would have to deal with individuals who use illegal technologies to steal the passwords of health care providers and thus obtain anonymous access to the health database. While credit card companies may protect itself and its customers with this type of fraud through insurance, it is impossible to recover potential harms once a patient’s private health record has been improperly accessed. Third, and arguably the most dangerous and worrisome, it is possible that the core network and database supporting the entire eHealth system is hacked into and the health data of Ontarians stolen. In July 2009, Alberta’s Netcare, Canada’s most developed provincial EHR, experienced a breach resulting from a virus, leading Alberta Health Services to send letters to over 11,000 patients whose medical, demographic, and/or financial information may have been breached. Although it is unclear whether patients’ health data was actually compromised and inappropriately accessed, this breach serves as a strong message to other provinces’ EHRs, including eHealth Ontario, that it must be vigilant in adopting strong security safeguards, including anti-virus software, as part of its plan to strengthen the privacy values behind the provincial EHR.

77 Charlie Dawes “Give the people control of online health records” The Ottawa Citizen (12 June 2009), online: The Ottawa Citizen <http://www.ottawacitizen.com/Health/Give+people+control+online+health+records/1687493/story.html>.

78 Ibid.

A recent study conducted at MIT and the University of Virginia looked at correlations between state medical privacy laws in the U.S. and the adoption of EHRs within a state, and found that an emphasis on privacy may decrease the rate of adoption of EHRs. The study suggested that the public has legitimate concerns about the privacy of EHRs and that individuals in states which had passed their own health privacy laws tend to be more interested in protecting their privacy. For example, they are more likely to sign up for the state’s do not call registry set up to combat telemarketing. Based on their findings, the authors also suggested that given the public’s concerns about maintaining the privacy of their electronic medical records, the government needs to take the lead in encouraging the adoption of this technology and explaining the long-term benefits to its citizens.  

2.4.3 Weighing the benefits and the harms

The benefits and harms associated with electronic health records give rise to what some authors have labelled as the “privacy paradox”. These authors argue that in order for a complex health care system to operate effectively, “a balance must be struck between protecting privacy and the need to use individuals’ personal health information”. As such, they claim that a paradox looms between Canadians’ demand for “high-quality, accessible and efficient health care and privacy for their personal health information”. In other words, there is a paradox between Canadians’ desire to ensure that they maintain their right to the highest quality of care


81 Upshur, Morin & Goel, supra note 73 at 307.

82 Ibid.

83 Ibid.
and accountability in the health care system while not compromising any privacy safeguards, such as the increased use of explicit consent.

Progress has begun to take place to ensure proper privacy protections are incorporated into EHRs. For example, Canada Health Infoway launched a new certification service in February 2009. This service is designed to ensure that emerging consumer health solutions provide adequate privacy and security provisions and can interoperate adequately with existing components of the EHR infrastructure currently being implemented across Canadian jurisdictions. Further, Infoway established a pan-Canadian Privacy Forum, with the objective of bringing together federal, provincial, and territorial privacy officers and health department representatives to discuss privacy governance matters as they relate to EHR management.

eHealth Ontario appears to be committed to protecting the privacy of Ontario’s electronic patient record. In its eHealth Strategy, 2009-2012, eHealth Ontario pledges to “provide patients with the means and the information necessary to participate in the management of their own care in a privacy-protective manner.” Further, in order to meet its privacy solutions, eHealth Ontario resolves to (1) complete the deployment of client, provider and user registries to ensure identity and access management in the clinical priorities (e.g. diabetes management, drug information system); and (2) develop a comprehensive provincial strategy for managing consent

---

86 eHealth Ontario, Ontario’s eHealth Strategy 2009-2012 (19 March 2009) at 5, online: eHealth Ontario <http://www.ehealthontario.on.ca/pdfs/About/eHealthStrategy.pdf> [eHealth Ontario, eHealth Strategy].
and implementing and enforcing consent directives for all eHealth solutions in compliance with the *Personal Health Information Protection Act (PHIPA)*.  

In the conclusion to its eHealth Strategy, eHealth Ontario acknowledges that risks to executing the strategy must be mitigated. Specifically, given that privacy and confidentiality of sensitive personal health information is a right under the law (i.e. *PHIPA*), privacy-related risks must be managed and privacy rights protected. The eHealth Strategy identifies the biggest risk to protecting these privacy rights as the uncertain legal environment in Ontario, given that *PHIPA* is currently under review, as required every three years. Although the Standing Committee on Social Policy has recommended amending section 73(1)(h) of *PHIPA* to allow for the creation of eHealth-regulated regulations, this process can be lengthy, especially given that the content and nature of these future regulations needs to be determined.  

In order to provide certainty to the legal environment surrounding privacy and electronic health records in Ontario, there needs to be a greater understanding of the definition of privacy in an electronic health environment. In Chapter 3, I will look at two different definitions of privacy in order to gain a better understanding of what factors must be considered in enacting change to the legislative environment in Ontario for electronic health records.

The general consensus behind the EHR discussion seems to be that the benefits of EHRs will outweigh their risks, and as such, Canada has taken steps to fund and legislate in this area.  

Further, eHealth Ontario needs to not only encourage the adoption of this technology, but also to explain to Ontarians why doing so will be in their long-term interest.

---

88 *Ibid.* at 44.  
89 Ries & Moysa, *supra* note 68 at para. 15.
A recent survey suggests that Canadians are generally supportive of electronic health systems that benefit health research and privacy protection and seem more willing to provide their personal health information for research purposes. Survey respondents showed the greatest support (85% to 89%) for using EHRs to study communicable diseases and quality of health care, and showed the greatest trust (78% to 80%) for data institutes, university researchers, hospitals, and disease foundations to conduct this research. Respondents were generally supportive of both research and privacy. Ninety percent of respondents were either somewhat or very concerned if allowing health research made it difficult to control how their information was being used. A similar percentage of respondents were somewhat or very concerned if protecting people’s rights to control access to their information made it difficult or impossible to conduct health research. Sixty-eight percent agreed somewhat or strongly with the statement: “Research that could be beneficial to people’s health is more important than protecting people’s privacy.”

In a separate recent survey conducted by Canada Health Infoway, Health Canada, and the Privacy Commissioner of Canada, close to nine in ten Canadians (88 per cent) supported the development of EHRs (up five percentage points since 2003) and recognized the benefits associated with EHRs, with access to patient information and improved efficiency as the most compelling reasons to support EHRs and concerns about security the lead reason for opposing EHR development. Further, with respect to the privacy and security of patient information, those seeing EHRs as better than a paper-based system outnumber those who see EHRs as worse by a margin of over two to one. Not surprisingly, those patients with firsthand experience with EHRs

---


91 Ibid.
(31 per cent of Canadians) are more likely to cite the benefits of this system, such as faster service and accessibility of health information. The following quote summarizes the essence of the majority of Canadians’ views on these issues: “If you can protect my privacy, I am okay with [electronic health records].”\footnote{EKOS Research Associates, “Electronic Health Information and Privacy Survey: What Canadians Think — 2007 – Executive Summary” (August 2007) at 6, online: Canada Health Infoway <http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_Electricit%20Summary_EN.pdf> [EKOS Research Associates].}
Chapter 3
A Framework for Understanding Privacy in an Electronic Health Environment

In order to determine the best legislative options for health information privacy in an electronic environment, we must understand privacy in three different ways – as a definition, as a value, and as a useful concept for determining privacy problems worthy of legal protection. First, I will look at the definition of privacy in the electronic health context. Specifically, I will examine two of the central definitions of privacy – control over personal information and limited access to the self – that are best suited to the protections in an electronic health environment and that best protect the values that privacy protects. Second, I will look at the values that these definitions of privacy protect in the electronic health environment, concentrating on the value that Canadians place on their privacy in the health care context and specifically in the emerging field of electronic health records (EHRs). I will focus on how autonomy, dignity, and personhood are values of privacy that are necessary to protect in the electronic health environment by looking at Canadians’ views, the Charter, and the common law. Third, I will use these definitions as the basis by which to examine privacy as a useful concept in the legal context in order to identify the privacy problems that deserve legal protection in an electronic health environment. Health information privacy in an electronic environment requires the protection of different privacy problems, as I will outline below. For example, individuals feel that they have lost control over their personal information when they are undergoing surveillance in an EHR environment. As such, surveillance is a privacy problem that is worthy of protection in legislation addressing the privacy of EHRs.

Once I have established this framework for privacy in an electronic health environment, I will apply this framework to different policy options for regulating privacy protections in an
electronic health environment in Ontario. In Chapter 4, I will examine three legislative options available to Ontario regulators by looking at how each option protects the definitions, values, and protections of privacy outlined in this chapter.

3.1 Definitions of Privacy in an Electronic Health Environment

The term ‘privacy’ is typically assumed to connote something positive, such as ensuring the privacy of one’s information or maintaining privacy in one’s home. The definition of privacy means many different things to different individuals, judicial bodies, and academics. Still, there are a few definitions of privacy that continue to be cited and explored, although not on an entirely frequent basis from a Canadian perspective.

In this section, I will examine two prominent definitions of privacy that demonstrate the importance of the protection of personal health information in an electronic health environment. While there are other ways of defining privacy, these two definitions best apply to this context. By looking at these definitions, we can gain a better understanding of the ways in which privacy is lost as electronic health records are implemented into the health care system. I will explore these definitions by examining how academics, theorists, and the judiciary have interpreted them and explain how they define the losses of privacy in an electronic health environment.

Both the Charter of Rights and Freedoms (the “Charter”) and the common law have strongly influenced the recognition and development of a definition of privacy. The Supreme Court of Canada has called the protection of privacy a central feature of the Canadian

---


Although the Charter does not specifically guarantee a right to privacy, this right underlies different Charter rights and therefore holds constitutional significance. For example, the section 8 right in the Charter “to be secure against unreasonable search or seizure” may be construed in terms of its underlying purpose, the protection of individual privacy. While this is not an absolute right, it protects an individual’s “reasonable expectation of privacy”, which ensures that an individual’s privacy interest is overridden by a superior government interest, the state must only be allowed to interfere in a “reasonable” manner. The purpose of section 8 has been identified as having “to protect individuals from unjustified state intrusions upon their privacy.” I will use the Charter and common law interpretations of privacy to explore the two different definitions of privacy in the sections below.

3.1.1 Privacy as control over personal information

The definition of privacy as “control over personal information” is one of the most central to Canadians’ desires to protect the privacy of their personal health information in an electronic environment. In exploring the meaning of privacy for Canadians, the federal Privacy Commissioner of Canada offered an understanding of privacy as “the right to control access to one's person and information about one's self.” She said that “[t]he right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses.” This definition suggests that for Canadians, privacy is about the right to control

97 Ibid. at 160.
99 Ibid.
their personal information and the right to choose when and how they may remain anonymous. Further, privacy is something that may be easily lost if not properly controlled.

According to Alan Westin, privacy “is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”100 Charles Fried, another leading proponent of this conception, defines privacy as “control over knowledge about oneself.”101 Fried contends that the notion that privacy is related to secrecy – to limiting the knowledge of others about oneself – must be refined. Privacy is not simply an absence of information about us in the minds of others; rather, it is the “control over knowledge about oneself.”102

In the context of health privacy, Lawrence Gostin advocates the definition of control over personal health information in his pioneering article on health information systems. Gostin notes that Americans’ views on health information privacy focused on the fact that they felt they had lost control over how their medical information is circulated and used. The element of control was seen as the most important priority in maintaining and protecting the confidentiality of medical records in order to advance national health care reform.103 He also emphasizes that since the most serious threats to privacy come from authorized users of health information, it is

100 Alan Westin, Privacy and Freedom 7 (New York: Atheneum, 1967) [Westin].
101 Charles Fried, “Privacy” (1968) 77 Yale L.J 475 at 483.
102 Ibid.
103 Gostin, supra note 70 at 453-454.
important to provide a reasonable measure of privacy for the individual by implementing some
control over the number of individuals who have access to health information.\textsuperscript{104}

Canadian courts have recognized, both at common law and under the \textit{Charter}, that every
individual has the fundamental right to control not only what may be done with his or her body,
but also the right to control – within reasonable limits – what is done with her or her personal
information in the health care context. At common law, an individual’s medical record is
recognized as a repository of highly private, personal information that is protected by legitimate
expectations of privacy and confidentiality.\textsuperscript{105} Further, the fiduciary nature of the doctor-patient
relationship supports the concept of control over personal information.

The Supreme Court of Canada has considered this definition of privacy in several
decisions. As early as 1928, the Court held that a patient’s \textit{prima facie} right to confidentiality in
the medical secrets kept between him and his physician was ‘‘absolute, unless there is some
paramount reason which overrides it.’’\textsuperscript{106} The Court noted that the fact that the disclosure of a
patient’s secret is made by one physician to another is not a decisive factor to justify it, although
in some cases that fact may have significance.\textsuperscript{107}

More recently, in the constitutional context in \textit{R. v. Duarte}, the Court described privacy
as ‘‘the right of the individual to determine for himself when, how and to what extent he will

\textsuperscript{104} \textit{Ibid}. at 485.

\textit{[McInerney]}. Patricia Kosseim & Megan Brady, ‘‘Policy by Procrastination: Secondary Use of Electronic Health

\textsuperscript{106} \textit{Halls v. Mitchell}}, \textit{ibid}. at 136.

\textsuperscript{107} \textit{Ibid}. at 139.
release personal information about himself.” This case demonstrated that the interest in being left alone by the state may be seen as including the ability to control the dissemination of confidential information.

Canadian courts have clearly and consistently held that individuals have a right to access information about themselves, subject to limited exceptions. In McInerney v. MacDonald, the Supreme Court wrote one of its leading decisions on health privacy in a civil suit involving the privacy of medical records. Although the case focused on access to privacy, McInerney demonstrated the judiciary's concern about an individual retaining some form of control over his or her personal information in the health care environment. In this case, a patient sought access from her physician to her medical records, including x-rays and test results prepared by other health care professionals. Some, but not all, of her records were provided to her. The Supreme Court held that patients have a right of access to their own records based on physicians’ fiduciary obligations toward their patients. La Forest J. noted that the patient confides highly personal and private information to the doctor and has a basic and continuing interest in what happens to that information and controlling access to it. In ordering that the entire file, including the disputed report, be provided to the patient, La Forest J. emphasized that an individual retains a “basic and continuing interest in what happens to [personal] information, and in controlling access to it” and that this interest continues even where the individual lacks any proprietary rights in the form of record.

La Forest J. analyzed the nature of a patient’s interest in the information contained in her health records as follows:

---

109 McInerney, supra note 105 at 148.
Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that go to the personal integrity and autonomy of the patient...such information remains, in a fundamental sense, one’s own, for the individual to communicate or retain as he or she sees fit.\textsuperscript{110}

In this decision, the Supreme Court affirmed that in the context of the patient-doctor relationship, the doctor must provide access to information, except in circumstances where such access would cause a significant harm to the patient. The Court also affirmed the patient’s continuing interest in and control of the information. The right of access established in this case has now been codified into Canadian privacy statutes, including Ontario’s \textit{Personal Health Information Protection Act} (PHIPA), as a legal right. Further, this case demonstrates that embedded in Canadians’ definition of health privacy is the right to control their personal information through their ability to access their health records; otherwise, they feel a loss in protecting their medical privacy.

One year later, the Supreme Court again analyzed “control over information” as the primary definition of privacy. In \textit{R. v. Plant}, the facts of the case focused on whether a search of a house with an alleged marijuana grow-up violated section 8 of the \textit{Charter}, whether the police check of electronic electricity bill records violated section 8, and whether, if any of these section 8 violations occurred, the evidence should be excluded under section 24(2) of the \textit{Charter}.\textsuperscript{111} In holding that section 8 was violated, the Court noted that the purpose of section 8 is to protect against intrusion of the state on an individual's privacy. Sopinka J. listed the factors to be considered in determining the parameters of the protection afforded by section 8 with respect to informational privacy:

\begin{itemize}
  \item \textsuperscript{110} \textit{Ibid}.
  \item \textsuperscript{111} \textit{R. v. Plant}, [1993] 3 S.C.R. 281 at 286.
\end{itemize}
Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allows for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.\textsuperscript{112}

In this decision, Sopinka J. put forward the common theory now adopted by the Supreme Court that informational privacy is said to protect one’s “biographical core of personal information.” He explained this view as follows:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the \textit{Charter} should seek to protect a \textbf{biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state}. This would include information which tends to reveal \textit{intimate details of the lifestyle and personal choice of the individual}.\textsuperscript{113}

Sopinka J. emphasized that although a person may feel compelled to disclose information about himself, he may nevertheless have a reasonable expectation that the information shall remain confidential to the persons to whom, and restricted to the purposes for which, it is divulged. To this end, the Court found that such reasonable expectations of confidentiality in personal information must be constitutionally protected.\textsuperscript{114} However, as discussed in further detail in section 3.1.2 below, the Supreme Court partially retreated from the ideal of a “biographical core” in the dog sniffer cases, \textit{R. v. Kang-Brown and R. v. A.M.}, where

\begin{itemize}
\item \textbf{112} \textit{Ibid.} at 293.
\item \textbf{113} \textit{Ibid.} [emphasis added].
\item \textbf{114} \textit{Ibid.} at 300.
\end{itemize}
the Court held that even though personal information does not go to the “biographical core”, it may still be worthy of protection.115

The Supreme Court reiterated this definition of privacy rights, with a focus on section 8 of the Charter, in another case surrounding a complainant’s medical records. In R. v. Mills, counsel for the accused obtained partial disclosure of therapeutic records and notes relating to the complainant that were in the possession of a counselling organization. The Court found that the “reasonable expectation of privacy or right to be left alone by the state protected by section 8 includes the ability to control the dissemination of confidential information.”116 Further, the Court held that the “values protected by privacy rights will be most directly at stake where confidential information contained in a record concerns aspects of one’s individual identity or where the maintenance of confidentiality is crucial to a therapeutic or other trust-like, relationship.”117

In the 2009 decision, R. v. Patrick, the Supreme Court dealt with the question of whether there is a reasonable expectation of privacy in our garbage. The Court held that Russell Patrick, a Canadian swimmer suspected of operating an ecstasy lab in his home, did not have a reasonable expectation of privacy in the items taken from his garbage. Therefore, the seizure of his garbage bags, the ensuing search warrant and the search of his home were lawful. The Supreme Court unanimously upheld the trial judge and Court of Appeal’s decisions that refused to agree with Patrick’s argument that the taking of his garbage bags by the police constituted a

117 Ibid. at para. 89.
breach of his right guaranteed by section 8 of the Charter to be free from unreasonable search and seizure. The court found that the reasonable expectation of privacy varies with the nature of the matter sought to be protected, the circumstances in which and the place where state intrusion occurs, and the purposes of the intrusion.\textsuperscript{118}

Binnie J., on behalf of the Court, discussed in detail the level of control that householders retain over the information found in their garbage. He concluded that householders retain this element of control as follows:

\textbf{[U]ntil the garbage is placed at or within reach of the lot line, the householder retains an element of control over its disposition and cannot be said to have unequivocally abandoned it, particularly if it is placed on a porch or in a garage or within the immediate vicinity of the dwelling where the principles set out in the “perimeter” cases such as Kokesch, Grant and Wiley apply. In municipalities (if there are any left) where garbage collectors come to the garage or porch and carry the garbage to the street, they are operating under (at least) an implied licence from the householder to come onto the property. The licence does not extend to the police. However, when the garbage is placed at the lot line for collection, I believe the householder has sufficiently abandoned his interest and control to eliminate any objectively reasonable privacy interest.}\textsuperscript{119}

This analysis by the Court in Patrick and in cases such as \textit{R. v. Dyment} which specifically address health information (discussed in section 3.2 below), raises the question of whether – through common law or legislation – similar boundaries can be drawn over how and when Canadians may control over their personal health information in their medical records. Given that Canadian courts have addressed this issue of controlling health information, it is up to legislators and policy makers to determine how to develop these boundaries in a consistent manner and in a way that advocates Canadians’ expectations in controlling these records.

\begin{flushright}
\textsuperscript{118} \textit{R. v. Patrick}, supra note 95 at para. 38.
\textsuperscript{119} \textit{Ibid.} at paras. 62-63.
\end{flushright}
Canadians’ views on the definition of privacy as control over personal information in the health care context may also be seen in a growing body of surveys on the topic. One study that focused on the use of personal information for health research showed that Canadians are supportive of health research but do not wish to completely relinquish control over the use of their personal health information. The study authors concluded:

Given the heterogeneity of consent choices, any long-run solution must take this into account to maintain public confidence in the confidentiality of the information they share with their physicians. Although the EMR may play a role here, the outstanding challenge is how best to elicit and keep up to date the individuals’ consent preferences. There are no easy solutions.120

In a recent survey conducted by Canada Health Infoway, Health Canada, and the Privacy Commissioner of Canada, the results showed that while Canadians’ enthusiasm for privacy laws may be high, overall low levels of familiarity with legislation in this area suggests that many may not be aware of their rights when it comes to the protection of their health information. Only two in five (39 per cent) Canadians have a clear or vague awareness of health privacy laws. In light of this, those surveyed felt that having the ability to control their personal information by finding out who accessed their health record and when – such as through the use of electronic audit logs – tops the list of ways to increase comfort levels (77 per cent say this would make them “more comfortable”). Further, 74 per cent felt that introducing new legislation that would make unauthorized access of personal health records a serious criminal offence would make them “more comfortable”.121 This demonstrates the importance of understanding Canadians’ views of health privacy when determining the best legislative route for electronic health systems.

120 Willison, supra note 90.
121 EKOS Research Associates, supra note 92 at 65.
This survey also demonstrated that Canadians are concerned about controlling and maintaining the security of their health information and would resist the use of their data without their consent, but have ambivalent attitudes towards the type of consent to be given. With respect to informed consent, 63% of respondents agreed that to “receive informed consent, health professionals would need to provide details of every anticipated use of health information”, while 71% agreed that to “receive informed consent, health professionals should not have to provide details of every anticipated use of personal health information on every occasion, but should be expected to make this information available on request and through pamphlets, brochures and other convenient means.”122 These attitudes demonstrate that Canadians believe that they can control their personal health information through consent mechanisms.

The analyses and judicial decisions examined above demonstrate that Canadian courts have clearly and consistently maintained that individuals have a reasonable expectation of privacy in and the right to control their personal health information and medical records, a right that undoubtedly should, has been, and will continue to be extended to health records in an electronic environment. This idea of controlling personal information is translated into provincial health privacy legislation, such as Ontario’s Personal Health Information Protection Act, 2004 (PHIPA), through provisions surrounding knowledgeable consent (see section 4.1.1 below for more information) to the collection, use and disclosure to personal health information and access to this personal health information, both important concepts which become increasingly complex in the context of enormous electronic health repositories controlled and accessed by multiple and varied health care providers.

122 Ibid.
As I will argue in Chapter 3 below, consent and access provisions must be included in the regulation of health privacy, regardless of the regulatory approach taken. The requirements to obtain consent prior to the collection, use, and disclosure of personal health information and to allow access to this information have become legal safeguards intended to proactively protect privacy and protect against unauthorized and unjustified intrusions. Based on the above discussion, it is clear that the definition of privacy as “control over personal information” is central to Canadians’ concerns surrounding and desires to protect the privacy of their personal health information in an electronic environment.

3.1.2 Privacy as limited access

The other major definition of privacy that resonates in the electronic health context is “limited access” to the self. Ruth Gavison, a leading proponent of this definition, states that privacy “is a limitation of others’ access to an individual” and is related to the amount of information known about an individual. This definition of privacy recognizes the individual’s desire to conceal himself or herself and to be apart from others. However, Gavison rejects the definition of privacy as a form of control over personal information because, in her view, the reasons we value privacy may have nothing to do with whether an individual has in fact chosen privacy.

The “limited access” definition of privacy may be seen as a more sophisticated form of the “right to be alone”, a definition put forward by Samuel Warren and Louis Brandeis in their

---

123 See e.g. Kosseim & Brady, supra note 105 at 17.
125 Ibid. at 427-428.
126 Solove, supra note 19 at 18.
famous law review article, “The Right to Privacy”. In this article, which has been seen as the foundation of privacy law in the United States, Warren and Brandeis determined that there was a separate, definable “right to be let alone”. They argued that the “right to be let alone” was a “general right to the immunity of the person, the right to one’s personality.” Warren and Brandeis contended that a right to privacy could be derived from the common law, and used the phrase “right to be let alone” from Judge Thomas Cooley’s famous treatise of torts to demonstrate that many of the elements of a right to privacy existed implicitly within the common law. Warren and Brandeis are seen as the first scholars to attempt to demonstrate that many of the elements of a right to privacy exist implicitly within the common law.

Warren and Brandeis’ article is also relevant to look at in the context of privacy and electronic health records in the 21st century because it began by describing how new technologies pose a potential threat to privacy. The new technology they focused on was the camera and its ability to take “instantaneous photographs”. Warren and Brandeis expressed concern over how this new technology would contribute to an increasingly sensationalist press, given the dramatic increase in newspaper circulation. This concern is similar to those concerns expressed by patients and privacy advocates with respect to the proliferation of electronic records in the health care context. Given the unknown potential impacts of this new, developing technology, there is a need to ensure that the individual’s right to privacy with respect to this new technology is properly considered and assessed in both present and future contexts. While Canadian courts

---

127 Ibid. at 16.
129 Ibid. at 193.
130 Solove, supra note 19 at 16.
131 Warren & Brandeis, supra note 128.
have explored the privacy as a tort, there has been no judicial recognition in Canada of a tort of breach of privacy, as Warren and Brandeis may have envisioned.\(^{132}\)

Gavison’s analysis goes beyond this right to be left alone. In defining privacy as “limited access”, Gavison’s objective was to define a “neutral concept of privacy” that is distinct and coherent because the reasons for which we expect and demand privacy in different situations are similar.\(^{133}\) In her view, individuals lose privacy when others gain physical access to them.\(^{134}\) She explains limited access as the common denominator of privacy as follows: “Our interest in privacy...is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention.”\(^{135}\)

According to Gavison, the definition of privacy as limited access is a complex of “three independent and irreducible elements: secrecy, anonymity, and solitude”.\(^{136}\) While each element is independent in that a loss of privacy may occur through a change in either one, the definition is coherent because they are all part of the same notion of accessibility and may coexist in the same situation.\(^{137}\)

One of these three elements, “secrecy”, is one of the most commonly associated words with “privacy”. Secrecy of personal information may be seen as a way to limit access to the self.


\(^{133}\) Gavison, supra note 124 at 423.

\(^{134}\) Ibid. at 433.

\(^{135}\) Ibid. at 423.

\(^{136}\) Ibid. at 433.

\(^{137}\) Ibid. at 434.
While the two terms are not synonymous, secrecy is often seen as a way of understanding the value of privacy. According to Daniel Solove, “the privacy-as-secrecy conception can be understood as a subset of limited access to the self.”\textsuperscript{138} The leading proponent of this conception of privacy is Richard Posner, an American judge who views privacy as an individual’s “right to conceal material facts about themselves”. As seen in the following passage, Posner views privacy as a form of self-interested economic behaviour, concealing true but harmful facts about oneself for one's own gain:

Much of the demand for privacy, however, concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person’s professed moral standards. And often the motive for concealment is ... to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit, as when a worker conceals a serious health problem from his employer or a prospective husband conceals his sterility from his fiancée.\textsuperscript{139}

Although Posner supports this definition of privacy, his analysis also critically implies that one of the problems with privacy is that concealment of information permits, to some extent, the misrepresentation of certain facts. As will be discussed later in this section, Posner’s example of a worker concealing a health problem from his employer demonstrates how secrecy is one of the privacy concerns that is addressed in health privacy legislation through provisions known as “lock-box” or “masking”.

Canadian jurisprudence surrounding adoption rights demonstrates the acceptance of secrecy as an important element of defining privacy in Canadian common law. In \textit{R. v. W. (D.D.)}, the British Columbia Court of Appeal recognized the “near paramountcy” of privacy

\textsuperscript{138} Solove, \textit{supra} note 19 at 22.

rights of an adopted child. Chief Justice McEachern stated: “I doubt if there could be any higher privacy right than that enjoyed by an adopted child at least until such time as she, having attained the age of majority, might decide to seek out her natural parents or one of them.”140 This suggests that an important aspect of the definition of privacy involves the ability to maintain the secrecy of certain discreditable information, which in this case involved samples of bodily fluids from a child allegedly born of the incestuous relationship.141

In Cheskes v. Ontario (Attorney General), the Ontario Superior Court of Justice addressed amendments to the Vital Statistics Act that would have far-reaching effects on adoption records.142 The amendments at issue would retroactively allow the Ontario government to disclose birth and adoption records without the consent of the birth parents or adult adoptees, contrary to the promise of confidentiality that had originally been made to them with respect to those records. Ms. Cheskes described her way of defining privacy as follows:

Registering to allow my identifying information to be disclosed to a birth-parent would have an enormous impact on the people closest to me in my life including my parents, my siblings and my daughter. By disclosing my identity, I am disclosing theirs, too. My family structure is very stable, strong and supportive and they have always encouraged me to make my own decision whether or not to seek or allow disclosure of personal information...The prospect of having to apply to a government board for a non-disclosure order that will only be granted in very limited circumstances is upsetting: My reasons for not wishing to seek out my birth family and wanting to keep my family information private are my own…I do not see why I should be forced to reveal this information or go through the stress and emotional turmoil of having to divulge these feelings to a board in the hope of then being allowed to keep my personal information private.143

141 Ibid. at para. 12.
142 Cheskes v. Ontario (Attorney General), 87 O.R. (3d) 581 [Cheskes].
143 Ibid. at paras. 31-33.
The Court found that these amendments violated the applicants’ right to liberty pursuant to section 7 of the *Charter*. The Court relied on past language used by the Supreme Court of Canada and found that the non-consensual disclosure of private records violated a privacy interest that extended beyond the actual documents themselves and impacted the dignity and self-worth of the individuals at issue. The Court held:

> [T]he disclosure of the birth and adoption records under the new law, in circumstances where a reasonable expectation of privacy has been created (recall the finding of fact above) constitutes an invasion of the dignity and self-worth of each of the individual applicants, and their right to privacy as an essential aspect of their right to liberty in a free and democratic society has been violated.\(^{144}\)

In coming to this conclusion, the Court referred to the Supreme Court’s reference to an “irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference.”\(^{145}\)

This case is particularly significant with respect to the definition of privacy in an electronic health environment and how such cases may be treated in the future for two reasons. First, Belobaba J. explicitly considered two safeguards that had been built into *Vital Statistics Act* – the no contact notice provision and the non-disclosure procedure. These are similar to provisions commonly found in provincial health privacy legislation to protect individuals against improper access to and disclosure of their health records. Specifically, the “lock-box” provisions of Ontario’s *PHIPA* enable individuals to control the access to and disclosure of personal health information by placing a “lock” on their records. Also similar to health privacy legislation, the administrative board at issue (the Child and Family Services Review Board)

---

\(^{144}\) *Ibid.* at para. 83.

could only grant a non-disclosure order in exceptional circumstances if it were satisfied that “the order is appropriate to prevent sexual harm or significant physical or emotional harm to [the adopted person or birth parent]”. Under PHIPA, adoptees and birth parents have the right to apply to the Child and Family Services Review Board for a non-disclosure order – a type of “lock-box” – that will be issued if certain pre-conditions are satisfied.

Second, the argument made by the Attorney General and the Court’s response may be indicative of how courts interpret health privacy and EHR-specific legislation in the future. The Attorney General argued that the ‘fundamentally personal decision’ line of cases did not apply to the case because the private information at issue was under the control of a government ministry, not the applicant. Belobaba J.’s responded as follows:

Strictly speaking, the decision whether or not to release the identifying information is the government’s, not the applicants’. I accept this distinction but I am more persuaded by the following two points – the first point was made by a Supreme Court judge and the second by an expert on adoption. First, that all information about a person is in a fundamental way her own, for her to communicate or retain for herself as she sees fit, and second, that the facts surrounding an individual’s adoption belong to that person regardless of where and how that information is stored. Furthermore, to say that the information is in the “control” of a government ministry begs the very question that’s before me.

Belobaba J. concluded that he could no reason why the government’s collection of personal information permits it to intrude on fundamental personal choices that would otherwise fall within the ambit of the liberty interest.

---

146 Cheskes, supra note 142 at para. 23.
148 Ibid. at paras. 88-89.
This case may shed light on what would happen if a legislative amendment that would retroactively open up confidential EHR records were challenged in Canadian court. As suggested by Patricia Kosseim and Megan Brady in the health research context, such an amendment could potentially remain vulnerable under a section 7 Charter analysis, even if a special procedure (e.g. lock box, masking) were built in to permit individuals to object to disclosure if the threshold for such a procedure were set too high.\(^{149}\)

*R. v. Patrick*, discussed above with respect to the definition of privacy as control over personal information, also values the definition of privacy as secrecy and concealment of information. Binnie J. summarized the court’s views on the concealment of information by referring to two 2008 Supreme Court decisions surrounding the issue of the reasonable expectation of privacy in police searches involving dog sniffers. Binnie J. explained as follows:

In *Kang-Brown*, we held that a traveller had a privacy interest in his carry-on bag despite the fact that the bag turned out to contain drugs. In *A.M.*, we held that a student did not forfeit his privacy interest in a backpack despite the fact that it was left unattended in a school gymnasium and that its contents included marijuana. In *Wong*, as stated, the Court held that people who “retire to a hotel room and close the door behind them have a reasonable expectation of privacy” (p. 50), despite engaging in illegal activity once inside. The issue is not whether the appellant had a legitimate privacy interest in the concealment of drug paraphernalia, but whether people generally have a privacy interest in the concealed contents of an opaque and sealed “bag of information”. I believe that they do. The focus is on “the person, place or thing searched and the purpose for which the search is undertaken” (*A.M.*, at para. 72). A warrantless search of a private place cannot be justified by the after-the-fact discovery of evidence of a crime.\(^{150}\)

This reasoning suggests that individuals may have a reasonable expectation of privacy when objects are concealed in an enclosed spaced in which each accused had a continuing expectation of privacy. Further, Binnie J. held that the fact that *A.M.*’s backpack was unattended at the time

\(^{149}\) Kosseim & Brady, *supra* note 105 at 41.

\(^{150}\) *R. v. Patrick*, *supra* note 95 at para. 32.
of the search did not remove his reasonable expectation of privacy in its contents. This suggests that the court is willing to go far to protect an individual’s reasonable expectation of privacy in situations where the individual believes that, after doing everything possible in the circumstances to conceal his items or information, he would maintain his level of privacy. In the context of health information privacy legislation, if an individual were to place a “lock box” or ask his physician not to share certain personal health information with others, then he would have a reasonable expectation that this information would in fact be concealed, even if he was not paying particular attention to the information at all times.

The idea of wishing to limit access to the self by concealing true but harmful facts is a widely-recognized principle in the health privacy context. Certain health privacy statutes embed this principle into a patient’s legislative rights, enabling a patient to conceal or block all or part of his or her personal health information from health care practitioners in certain circumstances. This principle is consistent with at least one survey, which demonstrated that a majority (55 per cent) of Canadians would find increased comfort levels with electronic health records if they were able to hide or mask sensitive information.¹⁵¹

For example, both Ontario’s Personal Health Information Protection Act, 2004 (PHIPA) and Manitoba’s Personal Health Information Act (PHIA) contain provisions known colloquially as “lock box”¹⁵². PHIPA provides the patient with a right to withdraw his or her consent to the collection, use, and disclosure of his or her personal health information for the purposes of health

¹⁵¹ EKOS Research Associates, supra note 92 at 65.
¹⁵² See further discussion of the lock box under section 4.1.1.
care and treatment.\textsuperscript{153} This right of a patient to invoke the “lock box” provisions is qualified in that patients do not have a right to withhold their consent from health information custodians who are using or disclosing their personal health information for purposes not directly relating to patient care and authorized to occur without consent. For example, health information custodians may use personal health information without consent for the purpose of risk and error management, and for planning or delivering programs or services.\textsuperscript{154} Similarly, individual health care providers may disclose health information without consent to a public health authority for the purpose of health protection and promotion (e.g. infectious disease reporting).\textsuperscript{155} These limitations on a patient’s right to withdraw his or her consent ensure that important objectives such as healthcare planning, management, and surveillance remain uncompromised.

Similarly, Section 22(1) of Manitoba’s \textit{PHIA} authorizes disclosures with an individual’s consent or without consent for the purposes listed in section 22(2) of the Act. For example, section 22(2)(a) of \textit{PHIA} states that trustees may only disclose personal health information to a person providing health care to the patient, unless the patient instructs the provider otherwise. Further, section 22(2)(h) authorizes trustees to disclose personal health information \textit{without individual consent} to a “computerized health information network and database” in which personal health information is recorded for the purpose of facilitating a health care program or research. However, as at least one commentator notes, it is unclear whether \textit{PHIA}’s lock box

\textsuperscript{153} Ontario PHIPA, \textit{supra} note 147, ss. 20(2), 37(1)(a), 38(1)(a), and 50(1)(e).

\textsuperscript{154} \textit{Ibid.}, ss. 37(1)(c) and (d).

\textsuperscript{155} \textit{Ibid.}, s. 39(2)(b).
provisions extend to an individual’s right to prohibit disclosure to an electronic health information network.\textsuperscript{156}

Based on the common law, Charter, and legislative approach to the definition of privacy as limited access, it is evident that the definition of limited access to the self is accepted in data protection regimes through requirements enabling individuals to conceal information about their selves and to maintain secrecy. By enabling individuals to limit access to their selves, health privacy legislation protects against unwanted privacy losses and intrusions, thereby promoting individual autonomy and dignity. In Chapter 4, I will look at how existing and potential legislative options best address the willingness, desire, and potential entitlement of individuals to be able to limit access to the most intimate details of their life in the electronic health environment.

3.2 The Values of Privacy in an Electronic Health Environment: Personhood, Autonomy, and the Preservation of Dignity

In order to understand why it is necessary to implement privacy safeguards into rules surrounding EHRs, it is important to understand the values underlying Canadians’ views on health privacy, electronic health systems, and related legislation. Without strong public and stakeholder approval for EHRs and the privacy protections surrounding them, Canadians will not buy into the idea of the EHR and their opinions and views must therefore be taken into account.

Privacy protects different values in different situations. Further, different ways of defining ultimately suggest that privacy often protects the same values regardless of its definition. For example, by defining privacy as a human right, we acknowledge that privacy is a

\textsuperscript{156} Ries, “Patient Privacy”, supra note 71 at para. 38.
moral and social value that not only extends beyond the protection of personal information, but that supports the development of individual dignity and autonomy. Recognizing these values, the Standing Committee on Human Rights and the Status of Persons with Disabilities acknowledged that “[p]rivacy is a core human value that goes to the very heart of preserving human dignity and autonomy.” 157 By adopting international covenants on human rights, nations recognize that privacy is a value that is not only beneficial to individuals, but also benefits society as a whole by strengthening individuals’ capacity for autonomy and dignity. 158

As defined above as control over information and as limited access, privacy in the health context best protects and embodies the values of autonomy, dignity, and personhood. According to one view, individuals desire privacy “out of a sincere conviction that there are certain facts about us which other people, particularly strangers and casual acquaintances, are not entitled to know...but instead [we] are to be respected as autonomous, independent beings with unique aims to fulfill.” 159 Further, this conception of privacy requires “a zone of relative insulation from

---

157 Ann Cavoukian, Ph.D., “Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation” (September 1999) at 4, online: Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/images/Resources/up-1pr_right.pdf>.

158 The conception of privacy as a human right may be seen in various international sources that recognize privacy as one of the fundamental human rights. Both the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) state: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” [see: Universal Declaration of Human Rights, 10 December 1948, A/RES/217, art. 12; International Covenant on Civil and Political Rights, 19 December 1966, 999 U.N.T.S. 171, art. 17, Can. T.S. 1976 No. 47, 6 LL.M. 368 (entered into force 23 March 1976, accession by Canada 19 May 1976)]. Although Canada signed the United Nations Declaration, it does not have privacy legislation that specifically addresses human rights. However, in Quebec, the Charter of Human Rights and Freedoms (1975) enshrines a right to privacy for residents and amendments to the Civil Code (1991) provide extensive privacy rights. See: Philippa Lawson and Mary O’Donoghue, “Approaches to Consent in Canadian Data Protection Law” in Ian Kerr, Valerie Steeves & Carole Lucock, eds., Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society (Creative Commons License, 2008) 23 at 24, online: On the Identity Trail: <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_02.pdf> [Lawson & O’Donoghue].

outside scrutiny and interference -- a field of operation within which to engage in the conscious construction of self."\(^{160}\)

The Supreme Court has most often characterized the values engaged by privacy in terms of autonomy, or the right to be left alone by the state. Autonomy may be seen as a value that is linked to the function of privacy in promoting liberty. In Gavison’s view, moral autonomy is the “reflective and critical acceptance of social norms, with obedience based on an independent moral evaluation of their worth”. Further, autonomy requires the capacity to make an independent moral judgment and the willingness to exercise it.\(^{161}\) When making decisions surrounding their privacy rights in the health care context and specifically in an electronic health environment, individuals value their ability to make decisions based on their autonomous moral judgment and their ability to exercise this autonomy.

In *R. v. Dyment*, Justice LaForest stated that “[g]rounded in man’s physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection.”\(^{162}\) In *R. v. Mills*, the Supreme Court recognized that the right to privacy has the same status as other *Charter* rights.\(^{163}\) In the famous Supreme Court of Canada case on abortion rights, *R. v. Morgentaler*, Madam Justice Wilson found, using a purposive interpretation, that the right to liberty contained in section 7 should be construed broadly to include a right over privacy decisions. She stated:


\(^{161}\) Gavison, *supra* note 124 at 449.

\(^{162}\) *R. v. Dyment*, *supra* note 12 at 427.

\(^{163}\) *R. v. Mills*, *supra* note 116 at para. 61.
[A]n aspect of the respect for human dignity on which the Charter is founded is the right to make fundamental personal decisions without interference from the state. This right is a critical component of the right to liberty...In my view, this right, properly construed, grants the individual a degree of autonomy in making decisions of fundamental personal importance.\footnote{R. v. Morgentaler (No. 2), [1988] 1 S.C.R. 30 at 166.}

Wilson J. concluded that “section 7 guarantees to every individual a degree of personal autonomy over important decisions affecting their private lives.”\footnote{Ibid. at 177.} As such, by limiting access to the self, privacy protects the individual value of autonomy, which is fundamental to the right of privacy that may be construed from section 7 of the Charter. When individuals exercise their right to make personal decisions, such as in the health care context, they feel a sense of autonomy that enables them to limit access to themselves and to intimate details of their lives. In turn, by limiting access to the personal information in their health records, individuals also maintain their sense of secrecy, anonymity, and solitude, which Gavison defines as the three independent and irreducible elements of the definition of privacy as limited access.\footnote{Gavison, supra note 124 at 433.}

While autonomy promotes an individual’s right to independence and liberty, dignity also protects an individual’s self-identity and personhood. Both autonomy and dignity promote an individual’s desire to define himself or herself. More specifically, these privacy values protect against conduct that is “demeaning to individuality” and “an affront to personal dignity”.\footnote{Edward J. Bloustein, “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser” (1964) 39 New York University L. Rev. 962 at 973-974, cited in Solove, supra note 19 at 30.} These values may also be seen as protecting “the individual’s interest in becoming, being, and remaining a person”.\footnote{Jeffrey H. Reiman, “Privacy, Intimacy, and Personhood” in Philosophical Dimensions of Privacy at 314, cited in Solove, supra note 19 at 30.} Further, these values of privacy embody the idea that an individual has
the right to experiment and make choices in an effort to define him or herself.\textsuperscript{169} Stanley Benn, a philosopher, contends that since surveillance restricts an individual’s range of choices and thus limits her freedom, privacy is ultimately about respect for personhood, with personhood defined as the individual’s capacity to choose.\textsuperscript{170}

In \textit{Dyment}, the Supreme Court addressed the constitutional right to privacy under section 8 of the \textit{Charter} as one that allows control over personal information and protects the values of autonomy and dignity. In this leading decision, the Court focused on the actions of a police officer who had obtained a vial of Mr. Dyment’s blood at a hospital from a physician who had taken the sample for medical purposes. Mr. Dyment had arrived at the hospital after being found in a vehicle with a head laceration. The officer did not have the patient’s consent to take the sample, nor did he have a search warrant. However, the officer proceeded to have the sample analyzed, found an excessive alcohol measure, and used this sample as evidence to charge Mr. Dyment with a \textit{Criminal Code} offence. The Court addressed the issue of whether the officer’s actions violated section 8 of the \textit{Charter}, and if so, whether it should be excluded as evidence under section 24(2) of the \textit{Charter} in criminal proceedings against the patient.\textsuperscript{171}

In one of the Supreme Court of Canada’s strongest commentaries on the right to individual privacy, the Court held that the officer’s seizure of the blood vial was unreasonable and that the patient’s privacy interests were violated. The Court found that the doctor did not have the right to use the blood samples for non-medical purposes or to give it to the officer

\textsuperscript{169} Bruyer, supra note 13 at 560.
\textsuperscript{171} \textit{R. v. Dyment}, supra note 12 at 421-422, La Forest J., concurring.
unless required by law, which would in itself be subject to Charter scrutiny. The Court was not willing to extend this Charter protection to the police officer for the purposes of taking an intimately personal substance (i.e. blood) from the physician, whose professional duty it is to respect the patient’s privacy. The Court noted that the easy flow of health information from hospitals presents a danger to an individual’s privacy, and therefore the police officer’s actions in taking the blood sample from the physician who had obtained it for medical purposes only was unreasonable in the absence of compelling circumstances of necessity.172

_R. v. Dyment_ suggests that the Supreme Court of Canada places strong importance on the protection of individuals’ right to control their personal information, especially in a health care setting. In his concurring opinion, La Forest J. referred to Alan Westin’s _Privacy and Freedom_ and held:

“Society has come to realize that privacy is at the heart of liberty in a modern state....Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual....The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.”173

La Forest J.’s words demonstrate that by being able to control their personal information, individuals are able to protect important values, namely their physical and moral autonomy and individual well-being.

In _Hill v. Church of Scientology of Toronto_, a Supreme Court decision involving a Charter challenge to the common law tort of defamation, Cory J. reiterated the constitutional significance of the right to privacy as protecting the values of autonomy and dignity.174 The

172 _Ibid._ at 426.
173 _Ibid._
Supreme Court has also emphasized that the liberty interest protected by section 7 of the Charter includes more than freedom from physical restraint. Rather, the liberty interest also protects the rights of citizens to make fundamental life choices without interference from the state and allows them to enjoy individual dignity and independence. To use the language used by the Supreme Court in Godbout v. Longueuil, the right to liberty in section 7 includes the “right to an irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference.”175 However, the only caveat is that the decisions being made must be fundamentally or inherently personal such that, “by their very nature, they implicate basic choices going to the core of what it means to enjoy individual dignity and independence.”176 This further suggests that an individual’s right to control his or her personal information protects the important values of autonomy and dignity.

The Supreme Court of Canada has also advocated autonomy, dignity, and personhood as significant privacy values in cases involving the production of medical records. In both R. v. O’Connor177 and M.(A.) v. Ryan178, the Court considered the issue of production of medical records in two different situations and addressed the potential impact of the production of medical records on an individual’s dignity related to the right under section 7 of the Charter. In O’Connor, L’Heureux-Dubé summarized the section 7 right to privacy in Canadian sources and jurisprudence and made a clear statement that a privacy interest is inherent in the right to liberty under section 7. She found that the “essence of privacy...is that once invaded, it can seldom be

176 Ibid.
"regained.” She went on to state the following about the disclosure of private information and its impact on a person’s liberty under s. 7 of the *Charter*:

In the same way that our constitution generally requires that a search be premised upon a pre-authorization which is of a nature and manner that is proportionate to the reasonable expectation of privacy at issue...s. 7 of the *Charter* requires a reasonable system of "pre-authorization" to justify court-sanctioned intrusions into the private records of witnesses in legal proceedings. Although it may appear trite to say so, I underline that when a private document or record is revealed and the reasonable expectation of privacy therein is thereby displaced, the invasion is not with respect to the particular document or record in question. Rather, it is an invasion of the dignity and self-worth of the individual, who enjoys the right to privacy as an essential aspect of his or her liberty in a free and democratic society.179

Two years later, in *M.(A.) v. Ryan*, L’Heureux-Dubé came to a similar conclusion surrounding the values of autonomy and dignity underlying the right to privacy found under sections 7 and 8 of the *Charter* when she stated: “That privacy is essential to human dignity, a basic value underlying the Charter, has also been recognized... Section 8 also reveals that the Charter is clearly premised on a respect for the interests of individuals in their privacy.”180

The Supreme Court echoed this view of privacy in discussing the reasonable expectation of privacy in a case involving bank records. In *Schreiber v. Canada (Attorney General)*, Lamer C.J.C. stated on behalf of the court:

This Court has said a great deal about how expectations of privacy, and their reasonableness, can be ascertained. In my view, the single most important idea that emerges from the jurisprudence is that expectations of privacy must necessarily vary with the context. This is inherent in the idea that privacy is not a right tied to property, but rather a crucial element of individual freedom which requires the state to respect the dignity, autonomy and integrity of the individual. The degree

179 R. v. O’Connor, *supra* note 177 at para. 119 [emphasis added].
180 *M.(A.) v. Ryan*, *supra* note 178 at para. 80.
of privacy which the law protects is closely linked to the effect that a breach of that privacy would have on the freedom and dignity of the individual.\textsuperscript{181}

The above-discussed decisions from the Supreme Court of Canada on the definition of privacy as a right to personal autonomy through control of information are consistent with a recent analysis conducted by Canadian business professors, Avner Levin and Mary Jo Nicholson, on privacy law in the U.S., the European Union, and Canada. The authors argue that the definition of privacy is focused on individual autonomy through personal control of information. In their article, the authors found that it is “Canada's coalescing identity as a multicultural haven that we perceive is the foundation of Canada's conception of privacy as autonomy protection.”\textsuperscript{182} Levin and Nicholson note that one of the fundamental values of a multicultural society – as opposed to either a traditionally homogenous society or a "melting-pot" society – is tolerance and respect for other members of society's autonomy and control of both their social and political characters. While a multicultural society does not attempt to impose values such as dignity or liberty on its members, it does encourage the autonomous development of these values within a multicultural framework. In essence, their research finds that Canadians perceive their privacy as most importantly protecting this autonomy, and believe that members of society should be free to decide for themselves what is important for them to control.\textsuperscript{183}

The United States Supreme Court has also recognized the right to privacy as a right that values personal autonomy and dignity in cases addressing choices such as reproductive rights,

\textsuperscript{181} Schreiber v. Canada (Attorney General), [1998] 1 S.C.R. 841 at para. 19 [emphasis added].

\textsuperscript{182} Avner Levin and Mary Jo Nicholson, “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground” (2005) 2:2 UOLTJ 357 at 393.

\textsuperscript{183} Ibid.
marriage, family relationships, and child rearing. For example, in Planned Parenthood v. Casey, the Court explained the constitutional right to privacy as follows:

“These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State.”

This statement suggests that the Court values the protection of privacy as the state’s non-interference in certain decisions that are essential to defining personhood. It is not difficult to argue that the concept of privacy as it relates to health care is “central to personal dignity and autonomy” given that health measures are taken on a daily basis for the prevention and treatment of disease. Dignity, autonomy, and personhood are undoubtedly important values to consider in determining the extent of privacy in the health care context. In this context, individuals desire these values because of the need to make important and often quick decisions and, in doing so, wish for their privacy to be respected and to not have information about themselves made available to others. This involves maintaining a level of autonomy in the decision-making process involving their health records, including being able to control the personal information found in these records.

The other definition of privacy discussed above, limited access, may also be seen as protecting the values of autonomy, dignity, and personhood. In her analysis, Gavison elaborates on the value of privacy and argues that privacy as limited access to the self is valuable in

---

185 Solove, supra note 19 at 31.
furthering liberty, autonomy, and freedom.\textsuperscript{186} This definition suggests that the right to privacy promotes respect for autonomy by “imparting to the individual a legal means of preserving and protecting his or her state of inaccessibility.” As such, “this protected sphere is an environment in which individuals can think and act voluntarily, unencumbered by the coercive influence of the outside world.”\textsuperscript{187}

Gavison claims that the best way in which to understand the value of privacy is to examine its functions.\textsuperscript{188} She explains the values protected by her definition of privacy as limited access to the self as follows:

We desire a society in which individuals can grow, maintain their mental health and autonomy, create and maintain human relations, and lead meaningful lives. The analysis above suggests that some privacy is necessary to enable the individual to do these things, and privacy may therefore both indicate the existence of and contribute to a more pluralistic, tolerant society. In the absence of consensus concerning many limitations of liberty, and in view of the limits on our capacity to encourage tolerance and acceptance and to overcome prejudice, privacy must be part of our commitment to individual freedom and to a society that is committed to the protection of such freedom.\textsuperscript{189}

Gavison’s overall analysis demonstrates that privacy is not only desirable as a definition and as a means of identifying losses, but also as a justifiable value.\textsuperscript{190}

Alan Westin, a leading U.S. privacy law scholar, may have best summarized these values encompassed by privacy when he wrote, “The most serious threat to the individual’s autonomy is

\textsuperscript{186} Gavison, supra note 124 at 423.
\textsuperscript{188} Gavison, supra note 124 at 441.
\textsuperscript{189} Ibid. at 449-450.
\textsuperscript{190} Gavison, supra note 124 at 459.
the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means.”191 As discussed in this section and as seen in cases such as Morgentaler and Dyment, control over personal information is necessary to protect individual autonomy and dignity. Individuals also wish to limit access to their selves in order to protect their autonomy and dignity. As such, when it comes to protecting individuals’ rights in the electronic health environment through regulation or legislation, we must consider the fact that individuals want to be autonomous, independent, and free from outside interference, particularly when it comes to controlling how they and others may access their personal health information.

3.3 Privacy Problems in an Electronic Health Environment

In his book, Understanding Privacy, Daniel Solove argues that since new technologies have generated a panoply of different privacy problems, a new taxonomy is therefore needed to address privacy violations for contemporary times. The purpose of his taxonomy is to aid the crafting of law and policy. Solove notes that while various attempts to clarify the meaning of “privacy” have been made, these attempts have not necessarily identified privacy problems in a comprehensive, methodical manner.192 In developing this new taxonomy, Solove argues that in order to understand the concept of privacy, one must look at the nature of the problem to which a privacy analysis is being attached.193 Solove contends that the law protects privacy in particular circumstances not because the particular activities are valuable, but rather to preserve the full range of activities that can be compromised by a particular type of privacy problem.

191 Westin, supra note 100 at 33.
192 Solove, supra note 19 at 101-102.
193 Ibid. at 99.
Dissatisfied with existing conceptions of privacy, Solove recognizes that in the present world of new technologies, a new taxonomy is necessary in order to address privacy issues for contemporary times. Solove’s taxonomy strives to provide “a more pluralistic understanding of privacy”\textsuperscript{194} and to provide a useful framework for the future development of privacy law.\textsuperscript{195} In focusing on activities that create privacy problems, Solove develops a taxonomy with four basic groups, each of which consists of related subgroups, of harmful activities: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion.\textsuperscript{196}

In this section, I will use the definitions of privacy discussed above – control over personal information and limited access – as the basis by which to identify the privacy problems that deserve legal protection in an electronic health environment. In doing so, I will examine certain privacy problems outlined in Solove’s taxonomy in order to determine which problems deserve protection in an electronic health environment. Given that Solove’s categorization considers the complexity privacy problems in contemporary times and provides a helpful framework for the future development of privacy law by focusing on the activities that create privacy problems, it is useful in assessing the privacy problems associated with EHRs, a contemporary issue with a myriad of potential issues. I will argue that the privacy problems and losses in an electronic health environment can best be determined on the two definitions of privacy in outlined in sections 3.1.1 and 3.1.2 above. As such, this section will outline how these two definitions of privacy function to help us see six different types of privacy problems and losses that occur in an electronic health environment and that are therefore deserving of

\textsuperscript{194} Ibid. at 101.
\textsuperscript{195} Ibid. at 102.
\textsuperscript{196} Ibid. at 103.
protection in legislation governing this environment. In examining these problems, I will demonstrate how the abilities to control personal information and to limit access to the self, respectively, are critical to the protection of autonomy, dignity, and personhood in an electronic health environment.

3.3.1 Control over personal information

In this section, I identify three types of privacy problems that may occur when individuals lose control over their personal information in an electronic health environment. If not properly addressed in legislation and policy, these three types of problems – surveillance, aggregation, and secondary use – could lead to losses of privacy that could potentially cause patients to not trust the collection, use, and disclosure of their personal health information in EHRs.

3.3.1.1 Surveillance

Control over personal information is necessary to protect individual autonomy and dignity against the privacy problem of surveillance. In his taxonomy, Solove describes “surveillance” as a form of “information collection”, which he explains as something that may create disruption, and even harm, through the process of data gathering, even if information is not publicly revealed. In an electronic health environment, individuals may be concerned that their personal health information will be inappropriately collected by the wrong individuals, such as health care providers, researchers, or government, or that personal health information will simply be improperly collected, either in excess or for incongruous purposes. Individuals feel that they have lost control over their personal information when they are undergoing surveillance in an electronic health environment. As such, surveillance is a privacy problem that is worthy of protection in legislation addressing privacy in an electronic health environment.
Surveillance may be seen as problematic in an electronic health environment in that it gives individuals the sense of being “watched by Big Brother”. As medical records are being transformed into electronic form, patients may be concerned that not only are their physicians seeing their personal health information, but this data may be shared with several health care providers, with various hospitals, and even with the government for unidentified purposes. Since surveillance can be overt or covert, individuals’ sensitive personal health information can be surveyed regardless of whether they are aware of the surveillance. In R. v. A.M., a recent Supreme Court of Canada decision, Binnie J. sought to alleviate concerns of today’s surveillance society as follows: “On these occasions, critics usually refer to 'Orwellian dimensions' and 1984, but the fact is that 1984 came and went without George Orwell's fears being entirely realized, although he saw earlier than most the direction in which things might be heading.”

The Supreme Court also expressed concern over the increased use of technological surveillance in R. v. Tessling, a case involving FLIR technology that allows authorities to obtain information about an individual’s private home using thermal imaging systems and infrared cameras. These cases demonstrate an increased recognition from the Supreme Court that surveillance of personal information is a reality that is continuing to grow and therefore must be addressed. However, these cases also revealed the Supreme Court’s position on addressing privacy and other concerns related to changes in technology, namely that such “concerns should be addressed

197 Ibid. at 106-107.
as they truly arise”. As such, while the Supreme Court has addressed health records in other cases, such as *Dyment* and *McInerney*, it is only likely to address privacy concerns surrounding EHRs as they arise.

When considering the harms associated with electronic health records, regulators must consider the losses caused by surveillance as a potential way in which individuals may lose control over their personal health information, with or without an individual’s knowledge. In order to ensure personal health information is properly collected, legislation regulating the electronic health record must contain technology-neutral privacy and security provisions, such as those focusing on audit logs, that limit the collection of personal health information to the minimum necessary means and that monitor this collection through the use of controls.

Regulators may also ensure that information is not inappropriately monitored by introducing mandatory requirements surrounding privacy risk assessment tools, such as privacy impact assessments. Certain legislation, such as Alberta’s *Health Information Act* (*HIA*), mandate the performance of these assessments in given circumstances, while other provinces rely on best practices or funding policies to determine when these assessments are conducted. For example, under the *HIA*, Alberta Health and Wellness must first perform a privacy impact assessment and submit it to the Information and Privacy Commissioner of Alberta prior to ordering custodians to share patient information. Alberta Health and Wellness must consider the Commissioner’s comments before issuing the order for custodians to share patient

---

201 *Ibid.* at para. 55. This reasoning was later adopted by the Supreme Court in *R. v. A.M.*, *supra* note 115 at para. 40.

202 *Health Information Act*, R.S.A. 2000, c. H-5, s. 46(1) (Alberta *HIA*).
information with Alberta Health. Further, organizations such as Canada Health Infoway require organizations to perform a privacy impact assessment as a condition of funding for electronic health record projects and, ultimately, as a way of preventing unauthorized collection of personal health information via these electronic systems.

3.3.1.2 Aggregation

Control over personal information is also necessary to protect individual autonomy, dignity, and personhood against another privacy problem, aggregation. Aggregation refers to the gathering of pieces of information about a person which, when combined, can create a greater picture about that person that he or she would not have anticipated when the original, individual pieces of information were collected. According to Solove, aggregation is part of the larger category of privacy problems identified as “information processing”. He contends that aggregation becomes increasingly problematic in a computerized environment because data is more easily collected, stored, and combined, with increasingly powerful technologies to analyze it. As such, we lose control over our personal health information when it is aggregated, thereby leading to losses of privacy.

In particular, in an electronic health environment, there is increased potential for data aggregation because patients’ personal health information will be collected from multiple sources and stored centrally for access by multiple health care providers and other organizations. For example, on a basic level, if a patient sees an oncologist about a potential form of cancer,

203 Ibid., s. 46(5).
205 Solove, supra note 19 at 118.
then his family physician could learn about potential conditions by viewing aggregated details about the types of tests performed. While this may ultimately lead to better care for the patient, he or she has no control over what, how, and when information is aggregated into the electronic health record. To this end, potential options for regulating the electronic health record must consider the aggregation of data and how aggregation may be used in a way that balances the need for this type of information with the patient’s desire to protect his or her information once it is in aggregated form.

3.3.1.3 Secondary Use

A further privacy problem that is necessary to protect through the control of personal information is secondary use. Solove also categorizes this problem under “information processing” and defines “secondary use” as the use of information for purposes unrelated to the purposes for which the information was initially collected without the consent of the individual to whom the information pertains.206 Potential secondary uses for electronic health data include public health surveillance, health system planning and management, quality assessment, health research, mandatory reporting, employment, insurance monitoring, drug marketing, and law enforcement purposes.207 Secondary use is a common problem identified in the EHR context because of the numerous ways in which individuals may lose control over their personal health information for uses that they did not consent to and may not have anticipated. In other words, individuals lose their sense of autonomy and dignity when they cannot control the ways in which their personal health information may be shared in an electronic environment.

206 Ibid. at 131.
207 Kosseim & Brady, supra note 105 at 6.
As will be discussed in greater detail in section 4.1.1 below, Ontario’s PHIPA, as well as other Canadian privacy legislation, recognizes the need to address the use of personal health information for secondary uses. For example, PHIPA anticipates health planning as a secondary use by including provisions for a “prescribed entity”. This is one approach used to address the problem that personal information may sometimes be used for secondary purposes, recognizing that it may be done in a way that properly protects personal information if guided by legislative limits. Given that the electronic health record will inevitably be used not only for primary uses (i.e. delivering health care) but also for secondary uses (e.g. research, health planning, pandemic preparation), any regulation of the electronic health record must address the variety of ways that electronic systems may or may not be used for secondary uses and how consent may be obtained for these uses.208

3.3.2 Limited Access

An advantage of the definition of privacy as limited access is that it allows us to conceptualize different types of privacy losses that individuals may suffer.209 As Ruth Gavison suggests, losses of privacy occur as others obtain information about an individual, pay attention to him, or gain access to him.210 In this section, I identify three types of privacy problems that occur when individuals are unable to limit access to their selves in an electronic health environment, thereby leading to an undesirable loss of privacy. In doing so, I will continue to define the scope of privacy problems that are necessary to protect individual autonomy and dignity in an electronic health environment. Specifically, I will look at how privacy losses that

208 For further discussion on secondary uses of electronic health records for health research purposes, see Kosseim & Brady, supra note 105.
209 Florencio & Ramanathan, supra note 187 at 82.
210 Gavison, supra note 124 at 428-429.
occur as the result of identification, breaches of confidentiality, and disclosures of information make us able to limit access to ourselves and to our personal information.

3.3.2.1 Identification

One type of privacy problem that occurs when individuals are unable to limit access to their selves, thereby leading to an undesirable loss of privacy, is “identification”. Identification has been defined as the “association of data with a particular human being”.211 In simple terms, identification allows us to determine the identity of a person. For example, DNA and fingerprints can uniquely identify individuals accused in criminal matters. In health care, patients are generally identified by a unique number, such as the Ontario Health Insurance Program (OHIP) number. In order to ensure accuracy, patients are often most identified using their first and last name, OHIP number, and date of birth.

The issue of the adequacy of de-identified information was recently examined by the Federal Court of Canada. The Court noted that “[i]nformation will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information”.212 As Solove notes, being asked to identify oneself is being asked to link oneself to data, not just to state a name.213 In an electronic health environment, this means that providing your name may inevitably lead to data linkage and identification beyond the initial purpose of the collection of personal health information. For example, researchers conducting a study on glucose levels in diabetes patients do not need access to the patients’ names, but rather only to that information

211 Solove, supra note 19 at 122.
213 Solove, supra note 19 at 126.
necessary to conduct reliable research. In this kind of situation, researchers may assign special numbers to the patients, with the assistance of a simple computer program, to identify them without having to see their names. This allows researchers to conduct accurate research and individuals to participate in these studies while knowing that they can limit how their information is accessed by others.

When individuals become identified – whether through a unique number or a combination of information – they enable further access to their selves. De-identification allows individuals to limit access to their selves, thereby protecting individual autonomy and dignity. As such, in order to allow individuals to limit access to their selves and to address privacy losses that occur when others gain access, legislation surrounding privacy in an electronic health environment should include provisions that distinguish between personal health information that is identifying and that which has been de-identified.

3.3.2.2 Breach of Confidentiality

The next two privacy problems that arise when individuals are unable to limit access to their selves occur as the result of what Solove calls “information dissemination”. Privacy problems arising from information dissemination occur when personal information is revealed or threatened to be revealed or spread, usually unknowingly or unwontedly. These problems stem from the fact that information that was considered private or confidential was somehow disseminated to the public, other health care providers, or simply other individuals. A breach of confidentiality is a privacy problem resulting from information dissemination that occurs when individuals are unable to limit access to their selves, thereby leading to an undesirable loss of

privacy. As Solove notes, protection against breach of confidentiality helps promote certain relationships (e.g. physician-patient) that build upon trust. Breach of confidentiality requires only a betrayal of trust, regardless of the nature of the data revealed.  

In a 2004 decision, the House of Lords addressed supermodel Naomi Campbell’s claim against a newspaper for breach of confidence after the paper published information about her drug therapy. The House of Lords addressed the distinction between privacy and breach of confidentiality. The Court held that Campbell’s claim for breach of confidence depended on the information in question being private, not public, information. As such, according to the UK’s breach of confidence tort, the test is whether disclosure of the information would give substantial offence to a reasonable person of ordinary sensibility placed in a similar position and faced with the same publicity. Once information is found to be private, a balancing exercise comes into play. In the US, tort law recognizes breach of confidentiality as a distinct harm that applies to, among others, the patient-physician relationship.

Further, just because information is broadcast to third parties does not mean that confidentiality has been lost or that the information is automatically in the public domain. An Alberta court addressed this issue in a case involving the disclosure of internal hospital documents on the performance of late-term abortions to a magazine editor. On hearing an

---

215 Solove, supra note 19 at 138.
216 Campbell (Appellant) v. MGN Limited (Respondents), [2004] UKHL 22 [Campbell].
217 Ibid. at para. 99.
218 Solove, supra note 19 at 140.
argument at an injunction that the magazine should be prevented from publishing an article with internal hospital information, the Court agreed and stated:

The fact that the defendants, or some other person, have already sent this information on to others does not make it knowledge in the public domain. The defendants cannot by their actions take something which is confidential and turn it into something which is not. It still retains its protection.\(^{220}\)

Canadian health privacy legislation sets out to protect against breaches of confidentiality by promoting a relationship of trust between provider and patient. For example, Ontario’s PHIPA relies on the “circle of care” to ensure that patient confidentiality is maintained. The “circle of care” enables health care providers to assume an individual’s implied consent to collect, use or disclose personal health information for the purposes of providing health care, subject to defined circumstances.\(^{221}\) PHIPA also protects against breaches of confidentiality by imposing requirements in the event of a breach of personal health information. PHIPA is currently the only Canadian legislation that establishes an unequivocal obligation to notify individuals if the security of their personal information is breached.\(^{222}\) Similarly, the United States’ new Health Information Technology for Economic and Clinical Health (HITECH) Act creates a federal security breach notification requirement for the U.S. health care industry, which applies to breaches of unsecured personal information held by health care companies.\(^{223}\)


\(^{221}\) Information and Privacy Commissioner/Ontario, “Circle of Care: Sharing Personal Health Information for Health-Care Purposes” (Fall 2009) at 5, online: Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/images/Resources/circle-care.pdf> [IPC, Circle of Care].

\(^{222}\) Ontario PHIPA, supra note 147, ss. 12(1), 12(2).

\(^{223}\) U.S. HITECH Act, supra note 1, s. 164.528.
When a patient’s confidentiality is breached, he loses his ability to limit access to himself and therefore loses his right to privacy. The legal protections described above – namely the circle of care and breach notification requirements – exemplify how legislation may provide individuals with some ability to limit access to their selves. To this end, legislation addressing privacy in an electronic health environment should protect against breaches of confidentiality in order to maintain a sense of limited access and to address privacy losses that occur when others gain access. Without protections surrounding breaches of confidentiality, individuals would not trust their health care providers or the use of electronic health records.

3.3.2.3 Disclosure

Another way in which information dissemination may cause privacy problems where individuals are unable to limit access to their selves is through “disclosure”. Solove explains that disclosure “occurs when certain true information about a person is revealed to others”. He notes that disclosure differs from breach of confidentiality because the harm in disclosure involves the damage to reputation caused by the dissemination, while the harm in breach of confidentiality is the violation of trust in the relationship. Once an individual’s reputation is harmed, he is no longer able to limit access to himself and risks losing his right to privacy. Without protections against the disclosure of personal health information, individuals will not trust how their information is used in the EHR.

In most consent-based health privacy legislation, including Ontario’s PHIPA, consent of the individual may be implied where the disclosure or sharing of information is to another

---

224 Solove, supra note 19 at 142.
custodian for health care purposes, unless the individual has expressly withdrawn consent.\textsuperscript{225} Disclosures may also be made without consent based on a number of exceptions, including the provision of health care services, disclosure to relatives and other interested parties, warning third parties of risk of serious harm, protection from abuse, judicial and quality review proceedings, public health, government purposes, and health research.\textsuperscript{226} Further, the nature of electronic information means that the improper disclosure of confidential health information can have further-reaching harmful consequences for patients than a breach involving paper records. An improper disclosure may lead to detrimental impacts on employment opportunities and health insurance coverage. A breach may also lead to social or psychological harms that can lead to stigmatization, social isolation, and a loss of self-esteem. For example, if a breach led to the discovery that an individual used a prescription drug associated with a certain condition (e.g. HIV-positive, erectile dysfunction), then that person could potentially lose current or potential employment opportunities or could be embarrassed in front of friends or family members who were not aware of this problem.

Further thought must be given to how health privacy legislation treats disclosures made in an electronic health environment for primary purposes now that these disclosures may be made with greater ease in the direct provision of patient’s care. Legislation must be clear about who has custody and control over personal health information at any given time and who is accountable for this information.

The privacy concerns surrounding disclosures of personal health information resonate with the concept of privacy as a public interest right. The Supreme Court of Canada has stated

\begin{footnotesize}
\begin{enumerate}
\item 225 Ontario PHIPA, supra note 147, s. 20(2).
\item 226 Gibson, Health Information, supra note 219 at 243.
\end{enumerate}
\end{footnotesize}
that the protection of privacy has “profound significance for the public order”. This conception of privacy differs from the other conceptions discussed in this chapter in that it focuses on the importance of privacy for the public good, as opposed to the individual’s personal needs. Ultimately, this concept of privacy must recognize and balance the dichotomy between the individual and the collective. This includes balancing the concept of personal autonomy underlying an individual’s right to control the collection, use, and disclosure of his or her personal health information against arguments about society’s interests in electronic health records for reasons such as health research, disease surveillance, or population health. Patricia Kosseim and Megan Brady argue that the protection of privacy may be as much a collective interest as it is an individual one. They point to the fact that the concept of public interest in the protection of privacy is finding increasing support in third generation privacy laws, including Ontario’s PHIPA and Alberta’s HIA. For example, PHIPA recognizes two competing interests in the health research regime, namely “the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed”.

When it comes to health privacy laws, it is not always clear which methods prevail for the public interest. In some cases, disclosing personal health information and enabling Canadians to access their records is in the public interest because it provides a sense of trust in government. In other cases, however, keeping personal health information confidential can also promote the public interest, especially in terms of encouraging Canadians to embrace and trust

---

229 *Ibid.* See: *Ontario PHIPA*, *supra* note 147, s. 44(3)(c); *Alberta HIA*, *supra* note 202, s. 50(1)(b)(i).
230 *Ontario PHIPA*, *supra* note 147, s. 44(3)(c).
electronic health records. As the Supreme Court stated in *Dagg*, requiring that a balance be struck between public interest objectives ensures that the goal of fostering openness and democratic accountability by providing access to public records does not trump a paramount interest in protecting the privacy of personal information.\textsuperscript{231} As such, future regulation of the electronic health record must take into consideration not only the individual interest in protecting personal health information, but the importance of the public interest in creating a trusting, capable approach to these records. This approach will allow individuals to limit access to their selves, thereby promoting the important privacy values of individual autonomy and dignity.

\textsuperscript{231} *Dagg*, supra note 11 at para. 97.
Chapter 4
Options for Regulating the Electronic Health Environment in Ontario

In this chapter, I will apply the framework developed in the previous chapter by looking at three policy and legislative options for proceeding with the regulation of electronic health records (EHRs) in Ontario. In doing so, I will assess the extent to which the current regulatory framework found in Ontario’s Personal Health Information Protection Act (PHIPA) is able to properly address the definitions of privacy described in section 3.1 and the privacy problems that these definitions protect in an EHR environment. I will highlight the inadequacies of this current health privacy legislation in properly addressing electronic health records, and will examine the varied approaches to EHRs in other existing health privacy legislation in Canada. By applying the framework developed in Chapter 3, I will assess the strengths and deficiencies of each of the three options in order to gain an understanding of the best direction for Ontario to take in regulating electronic health records.

As the Romanow Report suggested, there is a general lack of clarity about statutory privacy protections of personal health information in an electronic environment. As with many new and emerging technologies – such as radio-frequency identification devices, social media networks or cloud computing – the technology itself is way ahead of the applicable legislation, and lawmakers need to find a way to build laws that will stay current and practical and not become entirely obsolete as the technology progresses.

The four provinces with health sector legislation – Ontario, Manitoba, Saskatchewan, and Alberta – have each developed rules surrounding EHRs in their respective legislation. In some cases, those rules have been amended or new legislation has been introduced as providers and patients alike have gained experience with electronic health systems. Several provinces, including ones with and without existing health privacy legislation, have started to carefully consider the importance of a regulatory framework governing health information in electronic form. In general, these new frameworks show a trend towards protecting patient privacy, ensuring a patient’s right to access and control his or her personal health information, and promoting mandatory adoption of EHRs at a provincial level. It is important to note that this paper will not address the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*, since there have been no real efforts to amend this Act to accommodate EHR systems and since Ontario’s *PHIPA* has been deemed substantially similar to *PIPEDA* for the Ontario health care sector. While the federal government has committed funds for EHRS through Canada Health Infoway, this funding will flow to EHR projects across the country through provincial initiatives. To this end, it is important to focus on how individual provinces have reacted to regulating electronic health information through the legislative process.

I will now turn to the discussion of possible policy and legislative options that may be available to address the need that current health privacy legislation in Ontario does not properly address the accelerated pace at which EHRs are being introduced in the provincial, national, and

---

233 *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [PIPEDA].*
international health care landscape. I begin with the option of maintaining the status quo, which involves keeping Ontario’s *Personal Health Information Protection Act, 2004* in its current form. I then explore two alternatives to maintaining the status quo: (1) adopting Regulations to *PHIPA* that specifically address EHRs; and (2) introducing entirely new legislation that exclusively addresses EHRs, as has been done in British Columbia. In doing so, this chapter will summarize the strengths and weaknesses in *PHIPA*’s current approach to regulating health privacy in Ontario, which will eventually establish a pan-provincial EHR for Canada’s most populous province.

### 4.1 Option 1: Maintaining the Status Quo – The *Personal Health Information Protection Act, 2004*

The first policy and legislative option that I will address for ensuring proper privacy protections for the primary use and purpose of electronic health records is to maintain the status quo by leaving Ontario’s present health privacy legislation, the *Personal Health Information Protection Act* ("*PHIPA*"), in its current form. In order to understand this option, we must understand the current regulatory framework. As such, this section will begin with a history of the development of health privacy legislation in Ontario and will then critically assess how *PHIPA* currently addresses privacy in an electronic health environment by applying the framework developed in Chapter 3.
4.1.1 Background of PHIPA

Discussion surrounding the implementation of health privacy legislation in Ontario began with the Krever Report\textsuperscript{236} in 1980. A Royal Commission, headed by Mr. Justice Krever (as he then was), conducted an extensive review of the law pertaining to health information and inquired into its handling in health care facilities. The Commission documented cases of unauthorized access to health files maintained by hospitals and the Ontario Health Insurance Plan.\textsuperscript{237} In its review, the Commission found that the existing provincial legislation did not properly cover the issues surrounding personal health information, and where it did address it, the legislation was inadequate.\textsuperscript{238} The Krever Report concluded that comprehensive health privacy legislation was needed in Ontario.\textsuperscript{239}

Organized initiatives to draft health information privacy legislation began in 1996, with a Ministry of Health consultation paper. In 1997, the Ministry released the draft Personal Health Information Act, 1997, which provided a detailed legislative framework.\textsuperscript{240} Despite extensive consultation, this draft legislation did not succeed, but did serve as a strong precedent for

\begin{footnotes}
\item[239] Krever Report, \textit{supra} note 236.
\item[240] \textit{Ibid.} at 8-9.
\end{footnotes}
legislation developed in Alberta, Manitoba and Saskatchewan.\textsuperscript{241} Ontario attempted to introduce legislation in December 2000 with Bill 159; however, this bill died on the order paper.\textsuperscript{242}

The enactment of the federal \textit{Personal Information Protection and Electronic Documents Act (PIPEDA)}\textsuperscript{243} served as an impetus behind the implementation of \textit{PHIPA} in 2004. In 2001, Ottawa enacted \textit{PIPEDA} to establish national rules for personal information protection in the private sector and establishes, as law, the Canadian Standards Association Model Code for the Protection of Personal Information.\textsuperscript{244} As of January 1, 2004, \textit{PIPEDA} came fully into force in the health sector. \textit{PIPEDA} applies to every organization that collects, uses or discloses personal information, including health information, in the course of a commercial activity within a province, but will not apply where substantially similar provincial legislation is in force. \textit{PHIPA} came into force in Ontario in November 2004. In December 2005, the Ontario government declared \textit{PHIPA} as substantially similar to \textit{PIPEDA}.\textsuperscript{245}

\textit{PHIPA} governs the collection, use, disclosure, retention, and destruction of personal health information by health information custodians in both paper and electronic form. A health information custodian is a person or organization – specifically set out in section 3(1) of the \textit{Act} and under section 3 of the \textit{PHIPA Regulation} – who has custody or control of personal health information as a result of or in connection with performing the person’s or organization’s

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{242} Bill 159, \textit{An Act respecting personal health information and related matters}, 1st Sess., 37th Leg., Ontario, 2000.
\item \textsuperscript{243} \textit{PIPEDA}, supra note 233.
\end{itemize}
\end{footnotesize}
powers, duties or work. Some examples include a health care practitioner, a public or private hospital, ambulance service, specimen collection centre, and the Ministry of Health and Long-Term Care. Custodians are responsible for the practices of their “agents”, which includes employees, volunteers, and contractors. This means that it is possible for a physician to act as a health information custodian for the purposes of the management of his or her medical practice, and to also act as an agent of a custodian, such as a hospital.

PHIPA’s objective is to protect the personal health information of Ontarians by establishing a statutory privacy framework, with oversight authority for the Act under the Information and Privacy Commissioner of Ontario. The Act strives to balance the judicially recognized right to privacy with legitimate societal interests, a struggle faced in the balancing of all Charter rights. PHIPA reflects the consent-based approach to privacy, an approach often emphasized by the Supreme Court of Canada. PHIPA requires custodians to obtain an individual's consent for the collection, use or disclosure of an individual's personal health information, subject to some exceptions. The Act tries to balance the privacy interests of patients in the Ontario health care system against the need for efficient and timely sharing of their personal health information. It does so by allowing health information custodians to rely on implied consent and, in some cases, the “circle of care” for the sharing of health information.

Although the term “circle of care” is not actually used and therefore actually defined in PHIPA, it is a term commonly used to describe the ability of certain health information custodians to

---

246 Dyment, supra note 12 at 426.
247 See, generally, Ontario PHIPA, supra note 147, ss. 18-20.
248 Ibid.
assume an individual’s implied consent to collect, use or disclose personal health information for the purposes of providing health care, subject to circumstances defined in the Act.249

PHIPA also permits an individual to place restrictions on the use or disclosure of his or her personal health information by either expressly withdrawing or withholding consent. These sections of the Act, colloquially referred to as the “lock box” provisions, grant patients the right to prevent physicians from sharing locked personal health information internally.250 This right restricts the use of personal health information, whether the information was collected directly from a patient with consent or indirectly without consent because it was not possible to obtain timely, reliable or accurate information.251 Patients do not have an absolute right to restrict the use or disclosure of their personal health information. The “lock box” provisions generally do not override the provisions of PHIPA that allow uses and disclosures of personal health information without consent in certain circumstances, such as for risk management purposes, to find a substitute decision maker, to verify the eligibility of the patient to receive provincially-funded health care, and where a disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the person.252

In the next section, I will apply the framework developed in Chapter 3 in order to determine the viability of maintaining PHIPA in its current form as a regulatory option for legislating electronic health records in Ontario. In doing so, I will highlight some of the key features of Ontario’s current health privacy legislation and determine which aspects are working

249 IPC, Circle of Care, supra note 221.
250 The lock-box provisions are found in sections 20(2), 37(1)(a), 38(1)(a) and 50(1)(e) of Ontario PHIPA, supra note 147.
251 Ibid., s. 37(1)(a).
252 Ontario PHIPA, supra note 147, ss. 37(1)(d), 38(1)(c), 39(1)(a), and 40(1).
and which aspects need to be revised to address challenges arising from an electronic health environment.

4.1.2 Application of Framework to Option #1

4.1.2.1 Control over Personal Information

*PHIPA* enables Ontario patients to control their personal health information by: (1) requiring health information custodians to obtain consent, unless the Act permits or requires the collection, use or disclosure without consent; and (2) enabling patients to access their personal health information. Regardless of the regulatory approach taken, consent and access provisions must be a central part of health privacy legislation.

Under *PHIPA*, when consent – implied or express – is obtained for health care purposes in Ontario, it must contain the following four elements: 1) be of the individual; 2) be knowledgeable; 3) relate to the information being collected, used or disclosed; and 4) not be obtained through deception or coercion. Unlike earlier treatment models that focused on “informed consent”, *PHIPA* sets out a “knowledgable consent” model. Informed consent requires a custodian to provide the patient details about the foreseeable consequences of the decision to be made. While the informed consent approach is cumbersome when applied to the sharing of information, knowledgeable consent is easier on the custodian because it does not require the custodian to discuss the foreseeable consequences of consent. Under *PHIPA*, for consent to be knowledgeable, it must be reasonable in the circumstances for the custodian to believe that the patient knows 1) the purposes for the collection, use or disclosure; and 2) that he

---

253 *Ibid.*, s. 18(1).

or she may provide or withhold/withdraw consent. The custodian may meet this requirement by, for example, posting a notice or displaying a brochure in a conspicuous place in the office’s waiting room that includes, among other things, information on how a patient may provide, withhold, or withdraw consent.

The knowledgeable consent approach provides patients with control over their personal health information because it ensures that patients have a concrete understanding of the reasons for collecting, using, and disclosing their personal health information while not placing too high a burden on custodians to determine all reasonably foreseeable circumstances. Further, it provides patients with the opportunity to use this understanding to withdraw their consent from participating in some form of health care, whether it involves receiving a type of treatment or participating in an additional initiative undertaken by their health care provider.

PHIPA leaves specific rules regarding EHRs to be developed in the Regulations. Section 10(3) of the Act provides that “[a] health information custodian that uses electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any”. Section 73(1)(h) authorizes the prescription of regulations for the purposes set out in section 10(3) with which a health information custodian is required to comply when using electronic means.

However, there are currently no prescribed rules in PHIPA to provide guidance on consent and access in an electronic health environment. Instead, the Regulations prescribed under PHIPA with respect to electronic records focus on circumscribing the activities of those

---

255 Ontario PHIPA, supra note 147, s. 18(4).
256 Ibid. ss. 10(3), 73(1)(h).
who provide services to allow custodians to collect, use and disclose personal health information electronically. The Regulation defines a “health information network provider” as “a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another.” The Regulation also sets out several rules for the health information network provider, such as giving custodians a “plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.” The provider is also required to notify the custodian if there has been unauthorized access to information on the network, and to make available a public description of its services and security safeguards.

The PHIPA Regulation also provides specific guidance for eHealth Ontario (formerly the Smart Systems for Health Agency), the provincially-funded program dedicated to developing EHRs in Ontario. The Regulation requires the SSHA to put in place administrative, technical and physical safeguards that have been reviewed by the Information and Privacy Commissioner/Ontario. However, given the significant developments that have transpired with respect to EHRs and eHealth Ontario since PHIPA was brought into force in November 2004, this provision no longer provides sufficient guidance to providers who use electronic means on

257 Personal Health Information Protection Act, 2004, O. Reg. 329/04, s. 6(2) [Ontario PHIPA Regulation].
258 Ibid., s. 6(3).
how to properly collect, use, modify, disclose, retain and dispose of personal health information.\textsuperscript{259}

Although \textit{PHIPA} contemplates the ways in which patients may control and access their personal health information in a single-custodian, paper-based system and despite the fact that \textit{PHIPA} provides authority for rules surrounding EHRs to be developed in the Regulations, the \textit{Act} does not provide clear guidance as to how to deal with the issues of patient control and access in an electronic health environment. The \textit{Act} does not clearly outline who has custody and control – and is therefore accountable for – personal health information collected by multiple custodians in shared electronic health record repositories that function for the primary purpose of providing direct care to patients. Despite being the most comprehensive health privacy legislation in Canada, \textit{PHIPA} fails to contemplate how these electronic repositories may enable authorized health information custodians to access a complete picture of patients’ medical histories while obtaining implied consent only, and not express consent.\textsuperscript{260}

As \textit{PHIPA} presently stands, the regulatory framework does not sufficiently contemplate a pan-provincial EHR that functions for the \textit{primary purpose} of providing direct care to patients. While \textit{PHIPA} does provide specific rules regarding electronic health information databases that function for \textit{secondary purposes}, such as for the management of the health system and health research, it lacks clear rules governing shared electronic health record repositories for primary care. For example, \textit{PHIPA} and its Regulation classify certain organizations as “prescribed

\textsuperscript{259} Ibid., s. 6.1.

registries”, thereby empowering them to compile large electronic health records “for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances”. For example, the Cardiac Care Network of Ontario is a prescribed registry in respect of cardiac services and Cancer Care Ontario is a prescribed registry for the Colorectal Cancer Screening Registry.

Without consent provisions that enable individuals and custodians some control over the disclosure of personal health information into the provincial EHR, there is a lack of guidance on how some form of knowledgeable consent will be obtained, at the very least for the initial collection of personal health information that will be added to the EHR.

As discussed in section 3.1.1 above, cases such as McInerney v. Macdonald demonstrate that embedded in Canadians’ conception of privacy is the right to control their personal information through their ability to access their health records. Like most privacy legislation based on fair information practices, PHIPA allows individuals to have some control over their personal health information by codifying the right of access in most health care settings. PHIPA states that one of its purposes is “to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act”. Part V of PHIPA outlines the rules governing a patient’s access to his or her records of personal health information. In general, a patient has a right of access to a record of personal health

---

261 Ontario PHIPA, supra note 147, s. 39(1)(c).
262 Ontario PHIPA Regulation, supra note 257, s. 13(1).
263 Ibid., s. 1(b).
264 Ibid., ss. 51-54.
information about the patient that is in the custody or under the control of a custodian, unless one of the exclusions set out in the Act applies.

While PHIPA defines a “record” as any form, including electronic\textsuperscript{265}, it does not contemplate how individuals will be able to access their medical records from a provincial EHR. For example, it may be easier for individuals to gain access to this information from a centralized agency, whether at an organizational, regional, or provincial level – rather than leaving this administrative burden to individual physicians and hospitals. Although the details of the agency could be set out in policy or guidelines, rather than in legislation, PHIPA or other legislation could set out a basic framework, including the role of the custodian who originally created the information so that he or she could decide whether any of the exclusions or exemptions to the right of access provided for under PHIPA would apply (e.g. quality of care information, legal privilege).\textsuperscript{266}

In the 1980 Williams Commission Report, the Commission recognized that there are other ways to control personal information and recommended that individual control be achieved through notice to the individual of collection of personal information; direct collection from the individual; access to one’s personal information and right of appeal to an independent review body; right to correction or attachment of statement of disagreement; and onward disclosure of corrections to those to whom the personal information has already been disclosed.\textsuperscript{267} Although PHIPA contains provisions addressing these ways to control personal health information, these provisions must be reconsidered now that the personal health information at issue in PHIPA is

\textsuperscript{265} Ibid., s. 2.
\textsuperscript{266} Ibid., s. 54.
being stored mainly in electronic form, leading to new challenges for individuals, health care providers, and administrators. Any policy decisions made on the issue of consent must account for the lack of structure in existing legislation and must be consistent with any legislative changes.

4.1.2.2 Limited Access

*PHIPA* empowers individuals to limit access to their selves by maintaining the secrecy of their personal health information through what is colloquially referred to as the “lock box” provisions of *PHIPA*. These sections of the *Act* permit patients to place restrictions on the use or disclosure of his or her personal health information by either expressly withdrawing or withholding consent. In other words, these provisions grant patients the right to prevent physicians from sharing locked personal health information internally.\(^{268}\) This restricts the use of personal health information, whether the information was collected directly from a patient with consent or indirectly without consent because it was not possible to obtain timely, reliable or accurate information.\(^{269}\) However, patients do not have an absolute right to restrict the use or disclosure of their personal health information because the *Act* provides for certain circumstances when this information may not be locked.

It is not clear how the lock box provisions in *PHIPA*, which permit an individual to put a “lock” on their health record to decline consent for disclosure of personal health information to other custodians for purposes of care and treatment, are supposed to function in an electronic environment. When an individual imposes a lock box, his or her health care provider must inform the recipient of information about the lock box if the provider feels that not all

\(^{268}\) Ontario PHIPA, *supra* note 147, ss. 20(2), 37(1)(a), 38(1)(a) and 50(1)(e).

\(^{269}\) *Ibid.*, s. 37(1)(a).
information relevant to providing adequate care to the patient has been disclosed. However, the Act does not properly contemplate how a patient may be informed of his/her right to a lock box, given the non-personal nature of the EHR and the fact that an electronic environment may make a patient lose his or her ability to directly communicate with his or her health care provider. Specifically, the Act does not outline who is accountable for controlling the personal health information. For example, if a patient wishes to lock his/her information from certain health care providers, it is not clear who is responsible for ensuring this occurs and on what level of granularity.

As such, Ontario’s PHIPA would best enable individuals to limit access to their selves by clarifying the accountability structure and information governance framework for electronic health records. As will be seen under Option #2 (section 4.2 below), Ontario could look to existing models found in provincial health privacy legislation, such as Saskatchewan and Alberta, to clarify this framework. Alternatively, as discussed under Option #3 (section 4.3 below), Ontario could contemplate adopting new legislation specifically addressing electronic health records, such as B.C.’s E-Health Act, which contemplates an accountability framework and information governance structure for managing these electronic repositories on a provincial level. Regardless of the legislative approach taken, it must be consistent with policy developed by regulators and leaders at eHealth Ontario, which is responsible for developing consent management and information governance models for the province. These models should include, for example, direction on whether the lock box provisions should be expanded, how patient “opt-out” will be facilitated, and the level of granularity for an opt-out approach.

In addition to the consent, access, and lock box provisions of PHIPA that are undermined by privacy values, other PHIPA provisions show the value that the legislation places on
personhood, autonomy, and dignity. For example, *PHIPA* enables patients who are not able to consent to authorize another person to act on his or her behalf in a role known as a “substitute decision maker”. This may occur when the patient is mentally incapable, deceased, or is mentally capable but unable or prefers not to provide consent personally.\(^{270}\) *PHIPA* defines a “substitute decision maker” as a person who is authorized under the Act to consent on behalf of the patient to the collection, use or disclosure of personal health information about the patient.\(^ {271}\) Once authorized, the substitute decision maker has the same rights as the patient with respect to his or her health care. The substitute decision maker provisions in *PHIPA* serve an important role not only in protecting the patient’s privacy by respecting his or her dignity and autonomy, but also permits the substitute decision maker with some ability to maintain his or her dignity and autonomy when dealing with a difficult situation involving the health of a family member or friend who has died or who is or has become mentally incapable.

While *PHIPA* does not provide specific guidance on the role of substitute decision makers in an electronic health environment, the challenges facing a substitute decision maker in this new environment would not necessarily differ from those facing other patients. However, regulators should consider how substitute decision makers will be noted in the EHR so as to ensure that they have the ability to properly represent the patient’s rights.

### 4.1.2.3 Privacy Problems

In this section, I will assess how *PHIPA* currently addresses the privacy problems that I identified in Chapter 3 as being worthy of legal protection in an electronic health environment. I

---

\(^{270}\) Ontario *PHIPA*, *supra* note 147, s. 23(1).

\(^{271}\) *Ibid.*, s. 5(1).
will outline whether each of the identified problems are adequately covered by *PHIPA* and, if
not, how the failure to protect against these losses may weaken the current legislative framework.

When considering the harms associated with electronic health records, regulators must
consider the losses caused by surveillance as a potential way in which individuals may lose
control over their personal health information, with or without an individual’s knowledge. In
order to ensure personal health information is properly protected against unwanted surveillance,
any regulation of the electronic health record must contain technology-neutral security
provisions that limit the collection of personal health information to the minimum necessary
means and that monitor this collection through the use of controls.

In its current form, *PHIPA* and its Regulation provide limited guidance on security
standards, which are critical to a robust electronic health system. Presently, health information
custodians are required to “take steps that are reasonable in the circumstances to ensure that
personal health information in the custodian’s custody or control is protected against theft, loss
and unauthorized use or disclosure and to ensure that the records containing the information are
protected against unauthorized copying, modification, or disposal”.272 Further, custodians are
required to ensure that the records of personal health information in their custody or control are
retained, transferred, and disposed of in a secure manner and in accordance with any
requirements in the regulations.273 However, *PHIPA* does not contain any regulations imposing
specific security requirements.

---

While PHIPA’s requirements are technology-neutral and provide the varying types of custodians with flexibility, some more specific provisions would help custodians in establishing a security framework and in providing greater control over the personal health information involved in the EHR. As will be seen under Option #2 below (section 4.2), existing and proposed health privacy legislation in other Canadian jurisdictions provides better protection against the privacy problem of surveillance due to stronger provisions surrounding security safeguards. For example, PHIPA could better address surveillance and related privacy losses by including other technology-neutral provisions on access control, auditing or accounting of disclosures, authentication, and authorization. These provisions would benefit both the custodians responsible for implementing such technical safeguards and the vendors who design the software for EHR systems. Such provisions would enable a basic level of security to protect against unwanted and unnecessary surveillance of the EHR.

Another way to protect against the privacy problem of surveillance is through privacy impact assessments (PIA). PHIPA requires a “health information network provider”, an organization that provides services to multiple health information custodians so that they can share personal health information with one another, to conduct a PIA and to share the results of the PIA with the custodians who rely on the services.274 While PHIPA does not require a PIA to be conducted in any other circumstance, the Information and Privacy Commissioner/Ontario recommends that custodians perform PIAs in certain cases.275 Still, PHIPA could benefit from more requirements for PIAs in an electronic health environment which, in turn, would enable

---

274 Ontario PHIPA Regulation, supra note 257, ss. 6(2), 6(3)5.
organizations connecting to the EHR to have an adequate level of privacy and security and ensure individuals to feel a greater sense of control over their personal health information and a greater ability to limit access to their selves. For example, custodians could be required to conduct PIAs prior to joining the provincial EHR or prior to joining a specific system, such as the pharmacy drug network.

While PHIPA does not include provisions on privacy losses resulting from aggregation, it does recognize the need to address the use of personal health information for secondary uses. For example, PHIPA anticipates health planning as a secondary use by including provisions for a “prescribed entity”. Under the Act, a health information custodian may disclose personal health information to a prescribed person or entity “who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision or health care” or “for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services”. In order to become prescribed, such persons or entities must put in place practices and procedures to protect the privacy of the individuals whose personal health information they receive and to maintain the confidentiality of this information, and have these practices and procedures approved by the Information and Privacy Commissioner of Ontario. Once approved, a prescribed entity is permitted to use personal health information for a secondary purpose, namely research, as though it was a health information custodian under the Act, thereby imposing the same requirements for certain

---

276 Ontario PHIPA, supra note 147, s. 39(1)(c).
277 Ibid., s. 45(1).
278 Ibid., s. 45(3).
secondary uses of personal health information as for primary uses. Examples of prescribed entities include the Canadian Institute for Health Information and the Institute for Clinical Evaluative Sciences. This is one approach used to address the problem that personal information may sometimes be used for secondary purposes, recognizing that it may be done in a way that properly protects personal information if guided by legislative limits.

Although PHIPA contemplates, to some extent, secondary uses of electronic health records through its requirements for research, prescribed entities and registries, these designations demonstrate one-way flows of personal health information (i.e. into the electronic system, not between the provider and other providers or the patient). However, the legislation does not provide similar rules allowing authorized health care providers to access patients’ personal health information in EHRs without the patient’s express consent. In other words, PHIPA does not specifically contemplate authority for electronic systems for the purposes of compiling information to provide direct patient care. The failure to anticipate rules for this primary use of EHRs means that it is not always clear who has custody and control over patients’ personal health information once it is inputted into an electronic database.

Health privacy legislation, including Ontario’s PHIPA, addresses the privacy problems surrounding identification by distinguishing between “identifying information” and “de-identified information”. Under PHIPA, in order to constitute “personal health information”, the information must be “identifying”, which means information that identifies an individual or that it is reasonably foreseeable in the circumstances could be used, either alone or with other

---

279 Ontario PHIPA Regulation, supra note 257, ss. 13(4), 13(5), 18(3).
280 Ibid., s. 18(1).
281 Rodkin & MacPherson, supra note 260.
information, to identify an individual.\textsuperscript{282} Information may identify an individual in various ways, including by name, unique identifying number, address, biometric information, photographic information, or through a combination of information.\textsuperscript{283} The Canadian Institutes of Health Research (CIHR) notes that “data identifiability can be characterized as a continuum or sliding scale, in which the divisions between degrees of ‘identifiability’ and ‘anonymity’ are not always clear cut”.\textsuperscript{284} However, \textit{PHIPA} does not expand on what it means by “reasonably foreseeable” to identify an individual. It is commonly accepted that this term refers to circumstances in which information can be used to identify an individual when the recipient of the information is known to have access to other information that, when combined with the information that it received, would identify the individual to whom the information relates.\textsuperscript{285}

In contrast, \textit{PHIPA} defines “de-identified information” to mean “to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual”.\textsuperscript{286} Further, even though personal health information may become aggregated, as discussed above, this does not mean that it is not identifying. Personal health information is no longer “identifying” only when it is stripped of its identifying potential.\textsuperscript{287}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{282} Ontario \textit{PHIPA}, \textit{supra} note 147, s. 4(2).
\item \textsuperscript{283} Perun et al, \textit{supra} note 238 at 76.
\item \textsuperscript{284} Canadian Institutes of Health Research, Privacy Advisory Committee, \textit{Best Practices for Protecting Privacy in Health Research} (Ottawa: September 2005), online: Canadian Institutes of Health Research <http://www.cihr-irsc.gc.ca/e/29072.html>.
\item \textsuperscript{285} Perun et al, \textit{supra} note 238 at 76-77.
\item \textsuperscript{286} Ontario \textit{PHIPA}, \textit{supra} note 147, s. 47(1).
\item \textsuperscript{287} Perun et al, \textit{supra} note 238 at 78.
\end{enumerate}
\end{footnotesize}
Although *PHIPA* addresses the problem of identification, recognizing that it prevents individuals from limiting access to their selves, it does not directly address this problem in an electronic health environment. In fact, having EHR technology in place may make it easier for individuals’ identity to be de-identified, thereby allowing individuals greater ability to limit access to their selves and to protect their individual autonomy and dignity. Legislation surrounding privacy in an electronic health environment should address the specific challenges arising from identification and de-identification of EHRs.

*PHIPA* protects against privacy problems arising from information dissemination in several ways. First, the Act protects against breaches of confidentiality by promoting a relationship of trust between provider and patient. For example, Ontario’s *PHIPA* relies on the “circle of care” to ensure that patient confidentiality is maintained. The “circle of care” enables health care providers to assume an individual’s implied consent to collect, use or disclose personal health information for the purposes of providing health care, subject to defined circumstances. One of these circumstances is that the disclosure of personal health information by the health information custodian must be to another health information custodian.288

It is currently unclear how the concept of “circle of care” is supposed to apply in an electronic health environment, and *PHIPA* provides no specific guidance. In a September 2009 publication on the circle of care, the Information and Privacy Commissioner of Ontario gave no consideration as to how this often-misunderstood concept applies in an electronic health environment.289 In a digitized environment, it is more difficult and less intuitive for custodians

---

288 IPC, Circle of Care, *supra* note 221.
to assume implied consent. First, custodians are not required to communicate with one another in order to participate in a patient’s care and treatment in an electronic environment as they do when there is a real “circle of care”. Second, since not all health information custodians are entitled to assume implied consent, such as the Ministry of Health and Long-Term Care,\footnote{Ontario PHIPA, supra note 147, s. 20(2).} some of these custodians may still have access to patient information in the EHR even though they cannot imply consent. While the EHR would be able to log and record who accesses this information, patients may not feel the same sense of control as when they are aware who is in the circle of care. Finally, while custodians may only rely on assumed implied consent for the purposes of providing health care or assisting in the provision of health care to whom the personal health information relates, the electronic environment may enable custodians, and potentially non-custodians, to access this information without acknowledging the purpose for this access, thereby causing patients to feel less control over their personal health information in the EHR. Given the prevalence of EHRs and the looming goals of eHealth Ontario, Ontario health care providers require guidance – whether through legislation or policy – as to whether and how they can continue to assume implied consent in an electronic health environment.

*PHIPA* also protects against information dissemination by imposing requirements in the event of a breach of personal health information. *PHIPA* is currently the only Canadian legislation that establishes an unequivocal obligation to notify individuals if the security of their personal information is breached. The *Act* requires health information custodians to “take steps that are reasonable in the circumstances to ensure that PHI in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or
disposal.” Further, the Act imposes a duty, subject to exceptions, to “notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.”  

However, PHIPA does not contemplate how breach notification will work in an EHR environment. While the details of breach notification do not necessarily need to be legislated, it is important for health care organizations to know whether a single organization is in charge of notifying affected individuals so that individuals are not notified multiple times of the same breach, thereby feeling as if they are able to limit access to their selves. In this type of system, PHIPA could require the notifying organization to advise other custodians that notification has occurred. This type of legislative approach could be complemented by guidelines from, for example, the Information and Privacy Commissioner/Ontario and the Ontario Hospital Association.

While it is apparent that PHIPA addresses privacy in the three ways set out in the framework established in Chapter 3 – as a value, as a definition, and as a useful concept for determining privacy problems worthy of legal protection – it does not sufficiently contemplate the privacy problems associated with EHRs. Therefore, it is necessary to examine whether options for legislating EHRs in Ontario are better suited to addressing privacy in an electronic health environment.

4.2 Option 2: Amend PHIPA by creating EHR regulations

The second option for approaching the health privacy legislative scheme in Ontario to accommodate for EHRs is to amend Ontario’s existing legislation, PHIPA, by creating EHR-

---

291 Ontario PHIPA, supra note 147, ss. 12(1), (2).
specific regulations. This approach was recommended by the Standing Committee on Social Policy in August 2008, when the Ontario Legislative Assembly referred PHIPA to the Committee for a mandated legislative review. After oral and written submissions from stakeholders and the public, the Committee recommended, among other things, that section 73(1)(h) of PHIPA be amended to specifically “allow the development of a more comprehensive range of regulations related to e-health with a view to accelerating e-health initiatives”.292 Section 73(1)(h) currently allows the Lieutenant Governor to make regulations that require health information custodians using systems provided by health information network providers/service providers to follow “standards for transactions, data elements for transactions, code sets for data elements and procedures for the transmission and authentication of electronic signatures”. This approach was also supported by eHealth Ontario in Ontario’s eHealth Strategy, 2009-2012, where it recognized the need for eHealth-related regulations and expressed its commitment to working closely with Ontario’s Information and Privacy Commissioner and the Ministry of Health and Long-Term Care to ensure timely development of regulations required to support eHealth initiatives.293

Generally speaking, only an Act can amend an Act that is first enacted by way of a bill. This was the approach seen in Alberta, where the Alberta legislature introduced the Health Information Amendment Act in order to amend the Health Information Act (see section 4.2.1.1 below for further information). However, given the newness, complexity, and comprehensive scope of PHIPA, the legislation was designed with broad regulation-making powers. This

293 eHealth Ontario, eHealth Strategy, supra note 86 at 44.
enables the government to create regulations so that the Act can be fine-tuned on an ongoing basis, in a manner that properly protects privacy without disrupting existing processes and activities. While regulations are also laws, instead of being made directly by the Legislature, they are made under powers delegated by the Legislature, thereby enabling a quicker process. Although PHIPA was enacted by way of a bill, it may be amended by regulations, subject to certain restrictions outlined in the Act, in order to allow for an expedited process.\(^\text{294}\)

Given this broad regulation-making and in response to criticism about this process, legislators instituted several mandatory measures in section 74 of PHIPA in order to ensure a transparent and democratic process. These measures include the publication of a notice of any proposed regulations in the Ontario Gazette, allowing for a 60-day mandatory public consultation period. The Minister may shorten the consultation period or dispense with it with notice to the public on grounds of urgency or if it is a mere technicality or clarification of the Act. If the Minister dispenses with the public consultation period, the regulations are made in order to amend the Act without formal consultation. In this situation, the resulting regulation is temporary for two years before it expires, unless the Minister decides to consult the public to make it permanent. After the public consultation period closes, the Minister must report on any changes to the proposed regulation the Ministry considers appropriate. The Cabinet then makes the final determination on the content and passage of the regulation.\(^\text{295}\)

Despite the Standing Committee on Social Policy’s recommendations to amend PHIPA to add regulations specific to electronic health records, there are no such regulations being

\[^{294}\text{Perun et al, supra note 238 at 598-599.}\]
\[^{295}\text{Ontario PHIPA, supra note 147, s. 74.}\]
considered by legislators at the time of writing. In the next section, I will apply the framework developed in Chapter 3 to the option of amending PHIPA through regulations in order to determine whether this is a strong legislative and policy option for regulating electronic health records in Ontario. In doing so, I will look at approaches taken by other jurisdictions that have amended their existing health privacy legislation in order to accommodate EHRs.

4.2.1 Application of framework to Option #2

4.2.1.1 Control over Personal Information

By amending PHIPA to include EHR-specific regulations, the legislation would take a more proactive approach to regulating the protection of personal health information in an EHR environment. This would allow patients to have greater control over their personal health information in this environment by incorporating consent and access requirements specific to EHRs into the legislation. This approach has already been adopted by several other provinces, which have either amended their health privacy legislation or added additional regulations to ensure that individuals and health care providers better understood their rights and responsibilities with respect to protecting privacy in an EHR environment. This section will look at how these other provinces have updated and/or drafted their health privacy legislation in order to address EHRs and, in doing so, demonstrate ways in which Ontario could amend PHIPA to better regulate EHRs.

In Alberta, legislators are in the process of amending the province’s existing health privacy legislation, the Health Information Act (HIA), by enacting several amendments to the Act itself. Alberta’s Netcare, which links community physicians, pharmacists, hospitals and other

---

health care professionals across the province, is arguably the most developed and fastest-growing provincial EHR in Canada. As such, it is appropriate that Alberta is a provincial leader in health privacy laws and is the only province with both public health sector legislation (the HIA) and private sector privacy legislation (the Personal Information Protection Act).

Since its enactment in 2001, the HIA has undergone changes to those provisions dealing with EHRs. Section 59 initially required express consent from individuals before their health information could be disclosed by “electronic means”. However, this section was removed in 2003 based on feedback that compliance posed significant operational challenges. The Alberta Privacy Commissioner noted that in “facilitating a province wide [EHR], practical experience made it apparent that getting consent from Albertans was going to be difficult and costly.”  

Further, “it is [not] possible to inform people in a meaningful way, of all the specific disclosures by electronic means, which might ever be made of their health information.” This repeal demonstrates the lessons that may be learned from an onerous legislative requirement.

The accountability structure in Alberta’s HIA makes the custodian ultimately responsible for compliance. To illustrate, section 66(6) provides that despite the requirement for information managers to comply with the Act, the custodian continues to be responsible for personal health information disclosed to the information manager. This is a different approach than the current accountability framework in Ontario’s PHIPA, in which service providers are solely responsible, without any help from agents or other custodians. Further, PHIPA does not require agency agreements to govern relationships with its agents, as is the case in Alberta. The Alberta


298 Ibid.
governance structure provides stronger protection for patients’ electronic records and greater accountability measures than Ontario’s PHIPA, thereby giving patients greater control over their personal health information in the EHR.

In a 2004 review, a special committee appointed by the Alberta government considered the impact of EHRs on the HIA. This committee recommended that another legislative committee be formed to examine in detail the “need for more clear and transparent rules for the electronic health record.” In 2005, this new committee was struck and made a series of recommendations that formed the basis of a new Health Information Amendment Act, 2006. These amendments to the HIA address technical enhancements to provincial EHRs, clarify disclosure rules, improve the Ministry’s capacity to monitor drug trends, and enhance the privacy of Albertans’ health information. However, this new Act was not proclaimed into force.

In November 2008, the Alberta legislature introduced Bill 52, the Health Information Amendment Act, 2008, which would amend the HIA and, among other things, establish a mandatory legislative framework for a pan-provincial EHR. The bill also provides for the regulation of health information repositories, which may include local systems or small scale EHRs. The bill died on the order paper in February 2009, but was reintroduced as the Health

---


301 S.A. 2006, c. 18.


Information Amendment Act, 2009 in March 2009. The bill received Royal Assent on June 4, 2009, but has not yet been proclaimed into force.304

If proclaimed into force, Bill 52 would add Part 5.1 to the HIA in order to mandate participation in Alberta’s EHR. Part 5.1 mandates that custodians must make prescribed health information under its custody or under its control accessible to authorized custodians via the Alberta EHR. Making this information accessible does not constitute a disclosure of that information nor does it require the patient’s consent.305 The legislation would also require authorized custodians who use prescribed health information to keep an electronic log of the following information for 10 years: name or number that identifies the custodian who uses the information; the date and time the information is used; and a description of the information that is used.306 Further, individuals would be permitted to obtain a copy of the log that shows who has accessed their record.307 These audit log provisions are important with respect to ensuring that individuals have access to their health records and is a natural extension of the access requirements contemplated by the Supreme Court in McInerney. In determining its legislative approach and policy for the protection of EHRs, Ontario could mandate a similar approach that would provide individuals with greater access to, and therefore control of, their personal health information in the EHR.

305 Ibid. cl. 56.3.
306 Ibid. cl. 56.4, 56.41(1).
307 Ibid. cl. 56.41(3).
The mandatory approach to EHR participation made Bill 52 the subject of much debate surrounding the best way to respect the confidentiality of patient information and to allow for patient control over their information while facilitating a provincial EHR.\footnote{Anne Côté and Jane Steblecki, “Bill 52: Amendments to Alberta’s Health Information Act” Privacy Pages – Canadian Bar Association National Privacy and Access Law Section Newsletter (June 2009), online: The Canadian Bar Association <http://www.cba.org/cba/newsletters-sections/2009/2009-06_privacy.aspx#article1>.
} After legislative debate, Bill 52 was amended in order to satisfy concerns surrounding this EHR governance framework. First, Bill 52 originally stated that failure to comply would result in an offence and liability for a fine of up to $500,000. However, these provisions were amended to provide that if custodians fail to make listed health information available in the EHR, they will face disciplinary action. Second, the Bill was also amended to add provisions\footnote{Alberta Health Information Amendment Act, 2009, supra note 304, cl. 56.31.} that state that in deciding how much prescribed health information to make accessible via the Alberta EHR, a regulated health professional or authorized custodian must consider as an important factor any expressed wishes of the individual who is the subject of the information, as well as any other facts he or she considers important.\footnote{Alberta Legislative Assembly, Standing Committee on Health, “Report on Bill 52: Health Information Amendment Act, 2009” (May 2009) at 6, online: Legislative Assembly of Alberta <http://www.assembly.ab.ca/committees/health/PDF/Bill52_FinalReportSIGNED.pdf> [Alberta, Report on Bill 52].} This means that Albertans can ask that their health information be masked in Netcare.

Finally, Bill 52 now requires the Minister to establish a multi-disciplinary data stewardship committee to make recommendations to the Minister with respect to rules related to access, use, disclosure and retention of prescribed health information that is accessible via the Alberta EHR. This committee must contain at least two members of the public.\footnote{Ibid.} Given that a data stewardship committee is a trend also seen in British Columbia’s and Newfoundland,
Ontario should ensure that its legislative and policy approach to protecting the confidentiality of EHRs includes the establishment of such a committee.

Alberta Information and Privacy Commissioner Franklin Work initially criticized the provisions of Bill 52 relating to the EHR because they originally removed part of the patient’s consent and access rights that enabled them to adequately control their health information. Specially, the Bill initially removed the right of a patient to request that their health care provider consider the patient’s expressed wishes prior to disclosing information to the EHR and also removed the right of a patient to ask for a record of who is accessing their health information. However, Work has since expressed support for the Bill which, once amended, addresses his concerns. He stated that the amendments “address the key areas of concern I discussed in my original submission to the committee, and return a measure of privacy control for Albertans over their health information.”

Saskatchewan is another province that has updated its health privacy legislation in order to allow stronger patient control over personal information. Although Saskatchewan’s Health Information Protection Act (HIPA) has not been updated since 2003, it is still worthwhile to look at because it incorporated EHR provisions related to consent and access into its structure in a more direct way than Ontario’s PHIPA.


Under *HIPA*, patients exercise control over their information in the provincial EHR through the legislation’s consent provisions. When *HIPA* was implemented, it gave individuals the right to direct a trustee not to store their specified information on the Saskatchewan Health Information Network (SHIN), similar to the lock box provisions in Ontario’s *PHIPA*.\(^{314}\) Although this provision was removed in 2003, individuals retained the right to restrict who has access to their health record by giving written instruction to SHIN, with which SHIN is obliged to comply.\(^{315}\)

*HIPA* sets out a decentralized access model to regulate custody and control of for the provincial EHR. Under the Act, health care providers and other trustees have the power to authorize access to records they created, or if consent is deemed to exist or is not required.\(^{316}\) Individuals may exercise control over their health record in SHIN by stipulating restrictions on who may access their comprehensive health record via SHIN. Further, SHIN is required to provide a trustee with access to a comprehensive health record if each trustee whose records were used to compile the record has authorized access, and the patient has provided consent in writing authorizing the trustee to have access.

*HIPA*’s consent requirements therefore allow both individuals and trustees to exert some control over the disclosure of information through SHIN. This model enables the health care providers to understand who has custody and control over patient information in the provincial EHR, and also enables patients to have control over their information by requiring them to authorize trustees to access their records. Ontario’s *PHIPA* could learn from Saskatchewan’s

---

\(^{314}\) Saskatchewan *HIPA*, *supra* note 241, s. 1.

\(^{315}\) Saskatchewan *HIPA*, *supra* note 241, s. 8, as am. by S.S. 2003, c. 25; see Ries, “Patient Privacy”, *supra* note 71 at para. 41.

\(^{316}\) Saskatchewan *HIPA*, *supra* note 241, ss. 18.1(3), 27(2), and 27(4).
approach by incorporating consent requirements that enable individuals, services providers, agents, and health information custodians some control over disclosure of information into the provincial EHR. Although truly informed consent may be largely impossible to obtain from a patient regarding all the uses and disclosures of her information in an EHR, PHIPA should mandate knowledgeable consent for at least the initial collection of personal health information that will be added to the EHR in order to provide individuals with some control over their personal health information.317

In British Columbia, the provincial government took a novel approach to custody and control of personal information in an EHR by prescribing a regulation for its PharmaNet system, a network implemented in 1995 to link all pharmacies in the province into a central data system accessible by physicians, government, and emergency departments, providing them with patient medication history and comprehensive drug information.318 The PharmaNet system is one component of the provincial EHR. In 2004, the British Columbia government prescribed the Access to PharmaNet Patient Record Information Regulation319 under the Pharmacists, Pharmacy Operations and Drug Scheduling Act.320 Instead of regulating PharmaNet under specific privacy legislation, the government set out the privacy obligations for this electronic health system under this Act by providing legislative authority to access PharmaNet, and to record, use and disclose personal health information on the system. In its current form, the

317 For a further discussion of consent in the EHR context, see Ries, “Patient Privacy”, supra note 71.
PharmaNet Regulation\textsuperscript{321} limits which medical practitioners, persons, and regulatory bodies have access to the “limited personal health information”\textsuperscript{322} in PharmaNet. While Ontario may want to create more general EHR regulations for \textit{PHIPA}, the B.C. approach is a good example of how regulations may be enacted to allow for greater control and oversight of specific electronic health systems in a province.

\subsection*{4.2.1.2 Limited Access}

As mentioned under Option #1 above (section 4.1), \textit{PHIPA} does not clearly address how the lock box provisions are supposed to function in an electronic environment. By amending \textit{PHIPA} with EHR-specific regulations to address how these provisions should operate for the purposes of the provincial EHR, Ontario legislators could facilitate the ease with which the EHR functions and enable individuals to limit access to their selves. Both Alberta and Manitoba have attempted to address this issue by amending their respective health privacy legislation.

Manitoba’s \textit{Personal Health Information Act (PHIA)}, enacted in 1997 as one of Canada’s first health privacy acts, recognizes the importance of electronic health records in its preamble, which states that “clear and certain rules for the collection, use and disclosure of personal health information are an essential support for \textit{electronic health information systems} that can improve both the quality of patient care and the management of health care resources.”\textsuperscript{323} The \textit{PHIA} permits a trustee to disclose health information without consent to another person for the purposes of providing care to the subject individual, unless that individual has directed the

\footnotesize\textsuperscript{321} B.C. Reg. 117/2009.

\footnotesize\textsuperscript{322} Section 1 of the Regulation defines “limited personal health information” as in respect of an individual to whom drugs or devices are dispensed, any personal health information contained within the PharmaNet system except prescription claims information and supporting claims adjudication information.

\footnotesize\textsuperscript{323} Manitoba \textit{PHIA}, supra note 241 [\textit{emphasis} added].
trustee not to disclose the information to a computerized health information network that others may access for the purposes of facilitating care.\textsuperscript{324} This direction, which includes a list of permitted disclosures, constitutes the “lock box” provision of PHIA. As in Ontario’s PHIPA, the PHIA lock box provision empowers a patient to prevent disclosure of information to particular persons. However, it is unclear whether the right to restrict disclosure only applies to disclosure to a particular person, not to an electronic health information network that likely has multiple purposes, including facilitation of care delivery, program monitoring and payment.\textsuperscript{325}

As discussed above, Alberta’s Health Information Act presently contains a “global masking” provision. This differs from the lock box provisions found in Ontario’s PHIPA because the Alberta approach ultimately enables custodians to access personal information in the EHR for almost any reason through a specific protocol. In the report to the Standing Committee on Health regarding Bill 52, the Health Information Amendment Act, 2009, Laurie Blakeman (Member of the Legislative Assembly of Alberta) argued that the protection that a global mask offers for an individual’s privacy is insufficient and inadvertently misleading, thereby eroding public confidence in the confidentiality of Alberta’s health information system. She maintained that masking is not enough, and that Alberta should adopt the approach in Ontario’s PHIPA, which specifically provides an individual with the right to instruct his or her health care provider not to use or disclose his or her personal health information.\textsuperscript{326} However, despite her caution, Bill 52 was not amended according to her suggestion. Instead, the Bill mandates that custodians must make prescribed health information under its custody or under its control accessible to

\textsuperscript{324} Ibid., ss. 22(2)(a), 22(2)(h).1.
\textsuperscript{325} Ries, “Patient Privacy”, supra note 71 at para. 38.
\textsuperscript{326} Alberta, Report on Bill 52, supra note 310 at 8.
authorized custodians via the Alberta EHR. Making this information accessible does not constitute a disclosure of that information nor does it require the individual’s consent.\textsuperscript{327} After debate in the Legislature, the Bill was further amended to add the proposed section 56.31, which states that in deciding how much prescribed health information to make accessible via the Alberta EHR, a regulated health professional or authorized custodian must consider as an important factor any expressed wishes of the individual who is the subject of the information, as well as any other facts he or she considers important.\textsuperscript{328} This means that Albertans can ask that their health information be masked in Netcare, but only on a global level, and not on the single provider level.

As mentioned above, there has been strong criticism of the masking provisions proposed in Alberta. However, many of these criticisms were addressed through legislative hearings and several amendments were made in May 2009.\textsuperscript{329} The Alberta Information and Privacy Commissioner/Alberta initially criticized the provisions of Bill 52 relating to the EHR because they originally removed the right of a patient to request that his/her health care provider consider the patient’s express wishes prior to disclosing information to the EHR and also removed the right of a patient to ask for a record of who is accessing his/her health information.\textsuperscript{330} The Commissioner has since expressed support for the Bill which, once amended to permit health information custodians to use their discretion when submitting personal health information to the provincial EHR systems based on patient wishes, addressed his concerns.\textsuperscript{331} Although Ontario

\footnotesize{\textsuperscript{327} Alberta Health Information Amendment Act, 2009, supra note 304, cl. 56.3.}
\footnotesize{\textsuperscript{328} Alberta, Report on Bill 52, supra note 310 at 6.}
\footnotesize{\textsuperscript{329} Ibid. at 8-13.}
\footnotesize{\textsuperscript{330} Work, Presentation to Standing Committee, supra note 312.}
\footnotesize{\textsuperscript{331} Alberta Privacy Commissioner, Press Release on Bill 52, supra note 313.}
may not want to take the same global masking approach as has been taken in Alberta, it is worthwhile examining Alberta’s approach because it demonstrates that an approach to lock box or masking provisions may be developed while considering the provincial EHR. In order to enable Ontarians to limit access to their selves in an EHR environment, PHIPA’s lock box provisions must be revisited in order to account for a multiple custodian, pan-provincial EHR.

4.2.1.3 Privacy Problems

In this section, I will assess how PHIPA could be updated through EHR-specific regulations to better address the privacy problems worthy of legal protection in an electronic health environment. In doing so, I will examine how other Canadian provinces have dealt with some of these problems, and how PHIPA could learn from other legislation in order to improve its approach to protecting patient privacy in an EHR environment.

In amending PHIPA, Ontario regulators must consider the losses caused by surveillance as a potential way in which individuals lose control over their personal health information in an EHR environment. Since PHIPA currently only provides limited guidance on security standards, it could be amended to include security controls that limit the collection of personal health information and that monitor this collection through the use of controls. PHIPA could be amended to include more regulations surrounding EHRs and mandated security provisions in order to ensure greater control over personal information.

For example, Manitoba’s Personal Health Information Act (PHIA) requires trustees to adopt “reasonable administrative, technical and physical safeguards that ensure the
confidentiality, security, accuracy, and integrity” of personal health information.\textsuperscript{332} The Act requires trustees who maintain personal health information in electronic form to implement additional safeguards for this information. Specifically, trustees must put into place the following safeguards for electronic health records:

\begin{itemize}
  \item[a)] access controls that limit the persons who may use personal health information to those authorized to use it;
  \item[b)] authentication and identification controls to ensure that personal health information cannot be used unless identity and proper use is verified;
  \item[c)] network security controls and procedures to prevent the unauthorized interception of information transferred by electronic means; and
  \item[d)] controls to ensure that requests for disclosure of personal health information contain sufficient detail to uniquely identify the individual on whom the information is about.\textsuperscript{333}
\end{itemize}

Manitoba’s \textit{PHIA} also protects against surveillance by mandating the use of audit logs for electronic health records. The Regulation made under Manitoba’s \textit{PHIA} requires imposes a duty on trustees to create and maintain a record of user activity (i.e. an audit log) for electronic information systems used to maintain personal health information.\textsuperscript{334} The record of user activity may be generated manually or electronically.\textsuperscript{335} The trustee is required to meet these requirements in accordance with guidelines set by the Minister of Health.

While Manitoba’s \textit{PHIA} includes strong security safeguards for EHRs, it is outdated, due for renewed debate, and arguably lags behind Alberta and British Columbia in terms of innovation. Still, there has not been discussion in that province with respect to creating a new legislative framework specifically for EHRs, as in B.C., or in significantly amending the \textit{PHIA} in

\textsuperscript{332} Manitoba \textit{PHIA}, supra note 241, s. 18(1).
\textsuperscript{333} \textit{Ibid.}, s. 18(2).
\textsuperscript{334} \textit{Personal Health Information Regulation}, Man. Reg. 245/97, s. 4(1).
\textsuperscript{335} \textit{Ibid.}, s. 4(2).
order to mandate EHR participation, as in Alberta. However, the additional protections described above provide a secure environment in which to maintain personal health information in electronic records in Manitoba. Further, these provisions demonstrate to Ontario how technology-neutral security requirements may be built into legislation as new regulations governing a specific electronic framework under PHIPA.

As discussed under Option #1 above (section 4.1), PHIPA currently protects against privacy problems by mandating privacy impact assessments (PIA) for health information network providers. However, other jurisdictions more broadly mandate PIAs for electronic health systems in their health privacy legislation. Alberta, for example, uses a blended policy and legislative model. According to Alberta’s HIA, all custodians or affiliates who wish to connect to or access Netcare (the provincial EHR) must conduct a PIA.336 Netcare’s policy also requires custodians or affiliates to conduct an Organizational Readiness Assessment that assesses the organization’s ability to protect the privacy and security of individually identifying health information, execute an Information Manager Agreement with Alberta Health and Wellness, and to read and follow the Information Exchange Protocol (user agreement).337 Ontario could adopt a similar model to Alberta, such that all health information custodians who wish to connect to the provincial EHR are required to conduct a PIA and meet other appropriate requirements to properly protect the collection of patient information.

Saskatchewan’s Health Information Protection Act (HIPA), which came into force in September 2003, contains specific provisions specifically governing EHRs, or “comprehensive health records” that assist in addressing the privacy problems of surveillance and disclosure.

336 Alberta HIA, supra note 202, s. 64.
First, HIPA provides rules for “information management service providers”, who are individuals and organizations that process, store, archive, destroy or combine personal health information on behalf of the trustee or that provide information management or information technology services to a trustee with respect to records of the trustee containing personal health information. According to the Act, an information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for an authorized purpose.\textsuperscript{338} The Saskatchewan Health Information Network (“SHIN”) is an example of an information management service provider. HIPA allows SHIN to create these records, which compile personal health information from two or more trustees to create a full health history for an individual that may be accessed by other trustees.\textsuperscript{339} This approach defines who has custody and control over the electronic health records and allows individuals to control their personal health information by being able to access this information from a single source.

Another strong privacy protection built into Saskatchewan’s HIPA specific to EHRs is that trustees must enter into binding legal agreements with information management service providers, such as SHIN, before using the services of the provider. This ensures that the information is kept private and that the provider can only do as directed by the trustee.\textsuperscript{340}

Manitoba’s PHIA also protects against disclosure by providing for “information managers”, defined as “any person or body that processes, stores or destroys personal health information for a trustee or provides information management or information technology

\begin{footnotes}
\item[338] Saskatchewan HIPA, supra note 241, ss. 18(1),(3).
\item[339] Ibid., s. 18.1(1).
\item[340] Ibid., s. 18.
\end{footnotes}
services to a trustee”.\textsuperscript{341} The Act establishes specific requirements for information managers, including the requirement that a trustee must enter into a written agreement with an information manager that provides for the protection of the personal health information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.\textsuperscript{342}

Alberta’s HIA currently contains provisions that allow strong protection for electronic systems. Similar to Saskatchewan’s HIPA, the HIA creates a category of “information manager”, who may enter into an agreement with a custodian for electronic information.\textsuperscript{343} Once an agreement is in place, the custodian may disclose health information to the information manager without the consent of the individuals who are the subjects of the information. Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use or disclosure by the custodian.\textsuperscript{344} Further, any disclosure of health information to an affiliate of a custodian is considered a disclosure to the custodian.\textsuperscript{345} In other words, when a custodian enters into a relationship (whether contractual or otherwise) that involves the handling of health information by its affiliate(s), both the custodian and affiliate remain accountable for the information, thereby protecting against unwanted disclosure.

Ontario could take a similar approach to addressing disclosure problems by amending the regulations to PHIPA requiring health information custodians to enter into similar agreements

\textsuperscript{341} Manitoba PHIA, supra note 241, s. 1(1).
\textsuperscript{342} Ibid., s. 25.
\textsuperscript{343} Alberta HIA, supra note 202, s. 66(1).
\textsuperscript{344} Ibid., s. 62(2).
\textsuperscript{345} Ibid., s. 62(3).
with eHealth Ontario or other service providers in order to ensure that privacy and confidentiality provisions are built into the province’s electronic health systems.

Alberta’s HIA also imposes an obligation on custodians to maintain safeguards which must, for the security and confidentiality of records, address the risks associated with electronic health records.\(^{346}\) This obligation attempts to minimize privacy breaches and unwanted disclosures in electronic health networks. Alan Westin and Vivian van Gelder argue that in order to minimize EHR breaches, we must “construct a combination of protections – clear legal rules, stiff penalties for violators, application of biometric identifiers for both health-organization employees and individual patients, strong data system access and audit controls, wide use of encryption for sensitive data, an independent regulatory agency oversight of data-security practices, and provision of compensation for victims.”\(^{347}\) While this position may seem like an extreme approach for Ontario, privacy breaches are an inevitable risk to EHR systems, but do not necessarily always cause a loss. As Gavison contends, a loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him.\(^{348}\) Not every privacy breach causes these events to occur. For example, if a CD containing patient information is lost but no one finds it, a breach has occurred but a loss has not. To this end, Ontario’s PHIPA could better protect against privacy losses of surveillance and disclosure by looking to the HIA’s electronic safeguards provisions and amending the PHIPA regulations by

\(^{346}\) *Ibid.*, ss. 60(1), 60(2).


\(^{348}\) Gavison, *supra* note 124 at 428-429.
imposing clearer obligations and sanctions that will strengthen its safeguard requirements for electronic providers.

Although the legislative examples discussed above from Alberta, Manitoba, and Saskatchewan do not explicitly address the privacy problems of aggregation, secondary use, and identification, PHIPA could still be amended to include regulations surrounding these protections in an EHR environment. PHIPA does not currently contain provisions addressing losses resulting from aggregation. As such, regulators would have a clean slate from which to address this problem in EHR systems, where it is easier for aggregation to occur. While PHIPA presently addresses the problem of identification, recognizing that it prevents individuals from limiting access to their selves, the Act does not contemplate this problem in an electronic health environment, where it is arguably easier for individuals’ identity to be de-identified, thereby allowing individuals greater ability to limit access to their selves and to protect their individual autonomy and dignity. Ontario regulators could include provisions in an EHR-specific regulation under PHIPA that address the specific challenges arising from identification and de-identification of EHRs. For example, if individually identifying health information is to be disclosed via the provincial EHR, PHIPA could require that a separate consent be obtained from patients to disclose this information. Finally, in order to address potential losses arising from secondary uses of the EHR, PHIPA regulations could address the overall consent framework for these uses in the electronic health environment.349

349 For further discussion of possible policy options for addressing consent for research purposes in EHR systems, see Kosseim & Brady, supra note 105.
4.3 Option #3: Create new provincial legislation specifically addressing EHRs

Given the weaknesses of PHIPA in addressing EHRs and the current EHR climate in Canada, another option for regulating the protection of personal health information in electronic systems in Ontario is to introduce new provincial legislation that specifically addresses EHRs. Two other provinces – British Columbia and Newfoundland – have adopted different versions of this approach, as will be discussed in detail below. This approach would allow regulators to better contemplate, among other things, the role of eHealth Ontario into legislative requirements. In its current form, PHIPA does not properly contemplate the role that eHealth Ontario is set up to play in designing an electronic health system in Ontario and to set up systems that will enable a pan-provincial EHR, such as a client registry, chronic disease registries (e.g. diabetes), and drug, laboratory, and image repositories.

The Ontario legislature created eHealth Ontario by amending a Regulation under the Development Corporations Act. As a result of these amendments, the corporation previously known as the “Smart Systems for Health Agency” continues to operate under the new name of “eHealth Ontario”. The Regulation under the Development Corporations Act establishes eHealth Ontario’s mandate, which includes several objectives. One of these objectives is “to provide eHealth Services and related support for the effective and efficient planning,

---

350 Development Corporations Act, O. Reg. 339/08, amending O. Reg. 43/02.
351 Development Corporations Act, O. Reg. 43/02, s. 2(1).
352 Ibid., s. 1, defines “eHealth Services” as: “one or more services to promote the delivery of health care services in Ontario that use electronic systems and processes, information technology and communication technology to facilitate electronic availability and exchange of information related to health matters, including personal information and personal health information, by and among patients, health care providers and other permitted users”. 
management and delivery of health care in Ontario.\textsuperscript{353} Another objective specifically addresses privacy as follows:

“To protect the privacy of individuals whose personal information or personal health information is collected, transmitted, stored or exchanged by and through the Agency, in accordance with the \textit{Freedom of Information and Protection of Privacy Act, the Personal Health Information Protection Act, 2004} and any other applicable law.”\textsuperscript{354}

The Regulation also permits eHealth Ontario to collect, use, and disclose personal health information for the following specified purposes:

- To register individuals/organizations to use eHealth Ontario’s services;
- To verify the identity of individuals/organizations registered to use eHealth Ontario’s services; and
- To maintain and administer the registration of individuals/organizations registered to use eHealth Ontario’s services.\textsuperscript{355}

Currently, eHealth Ontario’s only roles under \textit{PHIPA} are as a service provider and network provider.\textsuperscript{356} These are limited roles that provide eHealth Ontario with specific responsibilities, such as an agent of the Ministry of Health and Long Term Care for carrying out various e-health initiatives. As part of its eHealth Strategy 2009-2012, eHealth Ontario pledges to complete the deployment of client, provider, and user registries to ensure identity and access management in its clinical priorities, namely diabetes management, drug information systems, and the Emergency Room/Alternate Level of Care initiatives.\textsuperscript{357} This section will discuss how Newfoundland and B.C. have each taken the approach of introducing new, EHR-focused legislation to enable and, in some cases, the e-health leaders to design a unique system that will

\textsuperscript{353} \textit{Ibid.}, s.3.1.
\textsuperscript{354} \textit{Ibid.}, s.3.3.
\textsuperscript{355} \textit{Ibid.}, s. 16(1).
\textsuperscript{356} Ontario \textit{PHIPA} Regulation, \textit{supra} note 257, s. 6.1.
\textsuperscript{357} eHealth Ontario, eHealth Strategy, \textit{supra} note 86 at 25.
transform health care delivery in their respective provinces. By applying the privacy framework developed in Chapter 3, I will assess the effectiveness of this option for regulating the protection of health information in Ontario’s e-health environment.

4.3.1 Background on Newfoundland’s Personal Health Information Act

Newfoundland and Labrador has paved the way among the Atlantic provinces as a leader in the governance of electronic health systems. While Nova Scotia and New Brunswick currently do not have health privacy legislation, both provinces are contemplating health privacy legislation intended to address personal health information stored in electronic form. Newfoundland’s Centre for Health Information, which is responsible for the development and management of a province-wide Health Information Network, recognizes that protecting the privacy of personal health information is central to meeting its mandate and works closely with the provincial health system to develop policies for the electronic collection, use, storage, and disclosure of personal information. In a recent publication, the Centre sets out its progress in developing an information governance structure for the provincial EHR. The Centre states that the elements of governance include clear direction to the governing body through legislation or Ministerial direction; a clear purpose for the governing body, which distinguishes between policy and operation; and the inclusion of stakeholders.

359 Newfoundland & Labrador Centre for Health Information, “About the Centre”, online: Newfoundland & Labrador Centre for Health Information <http://www.nlchi.nf.ca/about.php>.
Unlike Ontario, Newfoundland and Labrador did not have any health privacy legislation in place when provinces began to contemplate how their legislation could be updated to take into consideration developments with electronic health records. To this end, in May 2008, Newfoundland enacted (but has yet to proclaim into force) the *Personal Health Information Act*[^361], a provincial health privacy statute governing the collection, use, and disclosure of personal health information that protects the confidentiality of that information and the privacy of individuals with respect to that information, with a particular focus on electronic health records and the Newfoundland Centre for Health Information. Once proclaimed, the *Act* will apply to publicly- and privately-funded custodians[^362], as well as “information managers” to whom custodians may disclose personal health information for the purposes of processing, retrieving, storing or disposing of personal health information for custodians or who provides information management or information technology services to a custodian[^363]. Although the *Act* is similar to Ontario’s *PHIPA* in terms of its general structure, the *Act* specifically centres on rules for the creation of integrated records of personal health information (i.e. a provincial electronic health system) and pays greater attention to electronic systems than do the provincial health privacy statutes in Ontario, Manitoba, Saskatchewan, and Alberta.

### 4.3.2 Background on British Columbia’s *E-Health Act*

Ontario should also look to the approach taken in British Columbia with respect to regulating personal health information for electronic systems. Unlike Ontario, British Columbia does not have health privacy specific legislation and instead chose to look forward and enact

[^361]: S.N.L. 2008, c. P-7.01 [Newfoundland PHIA].
legislation specific to EHRs. The B.C. Act is different from the Newfoundland legislation in that while Newfoundland’s PHIA addresses health privacy both generally and with a special focus on electronic health records, B.C.’s legislation only applies to the regulation of electronic health repositories.

In May 2008, the B.C. government passed Bill 24 – E-Health (Personal Health Information Access and Protection of Privacy) Act (“E-Health Act”)364, with the goal of “giving citizens access to their health records and medical information, while strengthening privacy protection.”365 The E-Health Act received Royal Assent on May 29, 2008, but only certain provisions are currently in force.366 This Act made B.C. the first province in Canada to create a specific, standalone legislative framework governing access and privacy for electronic health information databases used for the primary purpose of providing direct care to patients, as well as other purposes. While most health privacy legislation, including Ontario’s PHIPA, includes some provisions about EHRs, the E-Health Act specifically designs privacy protections around EHRs.

The E-Health Act governs entire shared electronic health record repositories by enabling the creation of “health information banks” that authorize disclosure and use of personal health information for purposes other than those narrowly required for the diagnosis and treatment of


366 B.C. E-Health Act, supra note 364.
individual patients. Each bank is to be established by a designation order issued by the minister and is to be managed by a “health information bank administrator”. These administrators are responsible for managing the collection, use, and disclosure of personal health information via the health information bank in accordance with the minister’s designation order. Personal health information must be collected and used only for one or more of the established purposes set out, and must be disclosed only for one or more of the established purposes. These purposes include conducting or facilitating health research, preventing or managing chronic health conditions, facilitating health insurance and billing, and addressing public health threats. Further, the Act outlines offences for which persons or corporations may be liable for fines of up to $200,000.

If Ontario were to consider the same approach as B.C., it would involve designating organizations to create and manage shared electronic repositories of health information for daily clinical use by health care providers. The Diabetes Registry, which was announced to be at the centre of eHealth Ontario’s strategy, is an example of such a repository.

---

367 Ibid., s. 3.
368 Ibid., s. 3(1).
369 Ibid., s. 3(2)(b).
370 Ibid., ss. 4, 5, 21.
371 Ibid., s. 4.
372 Ibid., s. 24.
4.3.3 Application of Framework to Option #3

By creating new legislation focusing on EHRs and the protection of the health information found in the provincial EHR, Ontario would have the opportunity to create strong legal protections specifically addressing the unique challenges of EHRs. Although *PHIPA* provides a strong legislative scheme for health privacy in Ontario, legislators did not sufficiently contemplate the proliferation and impact of EHRs when *PHIPA* was enacted in 2004. As such, legislators may be able to better capture Ontarians’ definitions and values of privacy in an EHR environment by enacting brand new legislation. As has been done in Newfoundland and B.C., provincial EHR legislation may allow for a strong accountability framework and information governance structure for managing electronic repositories on a provincial level. While Newfoundland has introduced legislation that imposes direct obligations on its provincial e-health agency, the Centre for Health Information, B.C. has taken an approach of designating “health information banks” that are meant to allow for the delivery of systems through various electronic registries and repositories. This section will demonstrate how the option of creating EHR-focused legislation may allow for greater control of personal information, enable individuals to limit access to their selves, promote values of autonomy and dignity, and address several privacy problems leading to losses in an electronic health environment.

4.3.3.1 Control over Personal Information

Once enacted, Newfoundland’s *PHIA* will allow patients to control their personal health information by requiring express or implied consent relating to the provision of health care to the individual as part of a circle of care. Like Ontario’s *PHIPA*, consent must be knowledgeable, thereby providing patients with control over their personal health information by ensuring they
have an understanding of the reasons for collecting, using, and disclosing their personal health information.\textsuperscript{374} Newfoundland’s PHIA goes one step further than PHIPA by defining “circle of care” in the Act as “the persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.”\textsuperscript{375} This definition clarifies for individuals who is part of their “circle of care” and therefore enables them to feel a greater sense of control over their personal health information. Although this definition does not explicitly refer to how the circle of care relates to electronic health records, its language implies that the provision of health care and any necessary incidental activities would include information transmitted or accessed via electronic means.

Newfoundland’s PHIA also goes further than Ontario’s PHIPA in enabling control in that it directly contemplates custody and control of personal health information in the electronic environment. This is demonstrated in the “purposes” section of each Act. The purposes set out in Newfoundland’s PHIA are almost identical to those in Ontario’s PHIPA, but with two notable additions. Specifically, Newfoundland’s PHIA includes among its purposes: (1) the establishment of mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control; and (2) the establishment of measures to promote compliance with the legislation by persons having the custody or control of personal health information.\textsuperscript{376} Given that Newfoundland borrows almost identical language from Ontario’s

\textsuperscript{374} Newfoundland PHIA, supra note 361, ss. 23, 24.
\textsuperscript{375} Ibid., s. 24(3).
\textsuperscript{376} Ibid., ss. 3(d), 3(f).
Except for these two additions demonstrates that it was willing to learn from both the strengths and weaknesses of Ontario’s legislation. Ontario should now be willing to learn from its provincial counterparts.

PHIA directly contemplates custody and control by requiring custodians to disclose personal health information to an information network without the consent of the individual to whom the information pertains for the purpose of facilitating “the construction or creation of an integrated electronic record of personal health information in accordance with the regulations”. Further, PHIA designates the Newfoundland and Labrador Centre for Health Information as a custodian under the Act, thereby giving it wider legislative powers than, for example, eHealth Ontario. Given that patients do not have to provide consent for their health information to be disclosed, they may feel as though they are losing control. However, if the Centre were designated as an “information network” under the Act, this approach would allow for stronger control since the Centre would then have sufficient legislative authority to control the provincial EHR. In Ontario, eHealth Ontario is not currently granted this same level of custody and control from a legislative perspective under PHIPA, and any legislative changes need to take this omission or oversight into consideration.

Newfoundland’s PHIA also allows for greater control over personal information because it specifically contemplates the need to outline how individuals will access their personal health information in an electronic health environment. Under the Act, the Lieutenant Governor has the authority to make regulations concerning “records of personal health information in electronic

377 Ibid., s. 39(4)(c)(iii).
form”, including the procedure for responding to a request for access to or disclosure of a record of personal health information by a person outside the province. While these regulations have not yet been drafted and therefore cannot provide Ontario regulators with insight into how the process would work, the inclusion of this provision demonstrates recognition that it is important to provide special rules for individual access in an EHR environment.

B.C.’s new e-health legislation also provides for greater custody and control of personal health information in electronic health systems by specifically contemplating the governance structure for the collection, use, and disclosure of this information. Under the *E-Health Act*, the British Columbia Minister of Health may designate particular organizations as “health information banks” and establishes particular rights and responsibilities for these organizations. For example, the Minister could establish a health information bank for day-to-day clinical use by health care providers or for an imaging repository. If Ontario were to introduce new EHR-specific legislation, it could adopt a similar model by including requirements that permit the Ontario Minister of Health and Long-Term Care to empower particular organizations to administer shared electronic health record repositories, specify particular privacy rights and responsibilities for the designated organizations, and provide a wide range of health care providers with access to the repositories’ records for day-to-day clinical purposes. This would address a gap in Ontario’s health privacy legislative scheme by defining who is accountable for these electronic health systems and what an accountable party must do to protect the privacy of the personal health information that such a system contains. This approach would allow for

---

legislative requirements specifically designed to accommodate shared electronic health record systems used by health care providers in daily clinical use, which could further empower individuals to control their personal health information. 380

4.3.3.2 Limited Access

While PHIPA empowers individuals to limit access to their selves by maintaining the secrecy of their personal health information through the “lock box” provisions, it is unclear how these provisions apply in an electronic health environment. As such, Ontario could look at the model established in B.C.’s E-Health Act, which enables individuals to limit access to their information through “disclosure directives”. Under the Act, the Minister of Health must, through a designation order for a health information bank 381, authorize the making of disclosure directives by a person whose personal health information is stored in the health information bank. 382 The Minister has further authority to make regulations respecting the manner in which a disclosure directive must be made, the conditions that apply to the making or revocation of a disclosure directive, to whom a disclosure directive must be provided, and records that must accompany a disclosure directive. 383 A disclosure directive allows a patient (or his/her authorized personal representative) to request that all or parts of personal health information in his/her EHR be “masked” so that it cannot be disclosed without his/her express consent. Masking is a technique used in EHR systems to hide personal health information with “dummy data”, such as viewing *** instead of the actual information. The patient must provide this

380 Rodkin & MacPherson, supra note 260.
381 B.C. E-Health Act, supra note 364, s. 3 defines health information banks as databases of personal health information designated by the Minister to be a health information bank with specified responsibilities.
382 Ibid., s. 8.
383 Ibid., s. 26(2)(d).
express consent to an authorized user who has the appropriate permission to access the personal health information with consent (e.g. a health care provider).

In order for personal health information in the health information bank to be disclosed under B.C.’s *E-Health Act*, the health information bank administrator must enter into an information-sharing agreement with the recipient of the information, and the disclosure must satisfy the terms of the information-sharing agreement.\(^{384}\) Healthcare institutions and providers are required to disclose personal health information to the health information bank at the health information bank’s request, provided the request is authorized under the Act.\(^{385}\) While health information bank administrators are responsible for managing the collection, use, and disclosure of personal health information via the health information bank for most purposes, special data stewardship committees are responsible for managing disclosures of personal health information for the purposes of health system planning or research (i.e. health information bank administrators are responsible for all other purposes).\(^{386}\) In other words, patients will provide their implied consent for all of their health information to be included in the provincial EHR and are not allowed to choose not to participate in the EHR. However, patients may use disclosure directives to restrict which health care providers may access this information in the EHR. Should these health care providers wish to access this masked information, they must obtain express consent from the patient, except in emergency situations and when there is a serious risk of bodily harm.

---

\(^{384}\) *Ibid.*, s. 19.
\(^{385}\) *Ibid.*, s. 6.
\(^{386}\) *Ibid.*, ss. 11-18.
This ability to mask personal health information provides patients with the ability to limit access to their selves by restricting access to their information in the EHR. However, it is important to note that the consent directives sections of the Act are not yet in force, thereby leading to concerns that provincial EHR systems will be implemented without the right to mask information through disclosure directives. An organization, called B.C.’s Big Opt-out, has led a grass-roots movement to gain public support for several complaints with B.C.’s current consent model, including the ability of these directives to enable individuals to control what personal health information, if any, is maintained in the provincial EHR. This demonstrates a desire for citizens to be able to limit access to their selves through these disclosure directives.

4.3.3.3 Privacy Problems

The Ontario government has already recognized the benefits of Newfoundland’s PHIA in enabling control over personal information through the use of electronic safeguards. In the recent review of Ontario’s PHIPA, the Standing Committee on Social Policy stated that it “wishes to underscore the importance of accelerating e-health initiatives” and considered Newfoundland’s new health privacy statute as an example of a provincial attempt of doing so by providing comprehensive regulation-making powers concerning e-health matters. In referring to Newfoundland’s legislative approach in the review of PHIPA, Ontario has made positive steps to learning from other provinces’ innovative and potentially successful models. Specifically, the Committee referred to section 90 of Newfoundland’s Personal Health Information Act, which provides the Lieutenant Governor the authority to make regulations “respecting the creation,

387 B.C.’s Big Opt Out, supra note 76.
retention, disposition and reproduction of records of personal health information in electronic form, including integrated records of personal health information”\textsuperscript{389}, namely:

- The technology or process that shall be used to make or send an electronic record;
- The format of an electronic record, including the making and verification of an electronic signature;
- The place where an electronic record may be made or sent; and
- The time and circumstances when an electronic document is to be considered to be sent or received where it is considered to have been sent or received.\textsuperscript{390}

The Committee recommended that \textit{PHIPA} should be amended to allow the development of a more comprehensive range of regulations related to e-health with a view to accelerating e-health initiatives.\textsuperscript{391} Ontario could follow this recommendation by amending the Regulation found under \textit{PHIPA}, as discussed under Option #2 above (section 4.2), or by including these types of e-health provisions in new legislation focusing on e-health.

Although B.C. has introduced e-health specific legislation, it does not include these same types of security provisions in the \textit{E-Health Act}. One way in which B.C.’s legislative scheme protects against surveillance is by requiring privacy impact assessments (PIA) in the e-health context. B.C.’s \textit{Freedom of Information and Protection of Privacy Act} (FIPPA) requires the B.C. Ministry of Health Services to conduct a PIA regarding the proposed activities of any “health information bank” it established under the \textit{E-Health Act}.\textsuperscript{392} Further, the \textit{E-Health Act} permits a health information bank may enter into an agreement to provide an organization with patients’ information stored in the bank, so that the organization may use the information to

\textsuperscript{389} Newfoundland \textit{PHIA}, \textit{supra} note 361, s. 90(1)(i).

\textsuperscript{390} \textit{Ibid.}, s. 90(2)(a)-(d).

\textsuperscript{391} Ontario, \textit{PHIPA Review}, \textit{supra} note 292 at 10.

\textsuperscript{392} \textit{Freedom of Information and Protection of Privacy Act}, R.S.B.C. 1996, c. 165, s. 69.1(5)(a) [B.C. \textit{FIPPA}].
perform research or health system planning. Prior to a health information bank entering an agreement to provide patient information to an organization, the health information bank must perform a PIA to evaluate how providing the information may impact patient privacy. This approach prevents the unauthorized collection of personal health information via electronic systems, thereby attempting to mitigate against privacy losses associated with surveillance.

B.C.’s *E-Health Act* protects against the privacy problem of secondary uses by setting out rules for secondary uses of personal health information found in health information banks for purposes such as health planning, health research, and market research. For example, the *Act* forbids the disclosure of personal health information or information related to health service providers contained in a health information bank or ministry database for the purpose of market research. This suggests, for instance, that personal health information collected by pharmacists for the purposes of dispensing drugs could not be disclosed to a large market research company to collect information on patients’ spending habits. These secondary use provisions allow patients to have greater control of their information contained in health information banks because they know that their information will not be improperly disclosed for secondary purposes.

Should Ontario decide to introduce and enact EHR-specific legislation, it should establish a specific legislative scheme for breaches that occur in an electronic health environment. Given the unique nature of breaches in an electronic health environment, the option of enacting new,

---

393 B.C. *E-Health Act, supra* note 364, ss. 14, 15, 19.
394 B.C. FIPPA, *supra* note 392, s. 69.1(5)(b).
EHR-specific legislation provides Ontario with the opportunity to devise a breach notification framework specifically for breaches involving EHRs. While PHIPA has a mandatory breach notification requirement, this may not be necessary for breaches involving EHRs because it may be easier to assess whether actual harm occurred, such as when the personal health information involved is not encrypted. Such a breach notification framework could place responsibility on the person or organization that caused the breach to assess the risk of harm and to determine, possibly with the help of the privacy commissioner, whether notification is reasonable in the circumstances. Alternately, a framework could allow for central notification of breaches, such as by the privacy commissioner. Either way, a new framework should enable greater transparency in identifying breaches and in notifying the public of any harmful disclosures.

While B.C.’s E-Health Act does not directly contemplate breaches, Newfoundland’s PHIA provides a legislative framework for breaches that better considers the impact and structure of electronic health systems. Under PHIA, anyone who believes on reasonable grounds that a provision of the Act or its regulations has been or is about to be contravened can file a complaint, regardless of whether it involves their own personal health information or someone else’s.\(^{397}\) This right goes beyond most breach notification provisions and gives the individual both a strong sense of control over personal information and the ability to limit access to him or herself.

Further, unlike Ontario’s PHIPA, which imposes mandatory notification for all breaches, Newfoundland’s PHIA recognizes that it is not always necessary to notify individuals of breaches unless some sort of harm is involved. In general, the Act requires a custodian to inform

\(^{397}\) Newfoundland PHIA, supra note 361, s. 66(3).
the privacy commissioner of a breach where the custodian reasonably believes that there has been a material breach.\textsuperscript{398} However, this requirement does not apply where the custodian reasonably believes that the breach will not have an adverse impact upon either the provision of health care or other benefits to the individual who is the subject of the information, or upon the mental, physical, economic, or social well-being of the individual who is the subject of the information.\textsuperscript{399} This exception is important in an electronic health environment, where breaches can easily involve records of thousands of patients but without any risk of harm. At the same time, electronic health information can be illegally accessed from anywhere and transmitted across international borders quickly, cheaply, and with little risk of detection if proper oversight mechanisms are not in place. In the health care context, patients do not have any real recourse if a breach occurs and are unlikely to receive financial compensation for any loss. In other sectors, such as banking or retail, consumers may receive some financial compensation and also have the option of switching to a different organization. As such, Newfoundland’s \textit{PHIA} demonstrates greater vision into what potential issues may arise when it comes to protecting against losses associated with breaches and disclosures in an electronic health environment.

The United States \textit{Health Information Technology for Economic and Clinical Health (HITECH) Act},\textsuperscript{400} part of the U.S. economic stimulus legislation passed in February 2009, also contemplated how breach notification would work best in an electronic health environment. HITECH amended the \textit{Health Insurance Portability and Accountability Act of 1996} (HIPAA) to, among other things, require covered entities to notify all individuals whose information is the

\textsuperscript{398} \textit{Ibid.}, s.15(3).
\textsuperscript{399} \textit{Ibid.}, s.15(5).
\textsuperscript{400} U.S. \textit{HITECH Act}, supra note 1.
subject of a breach when a breach poses a significant risk of financial, reputational, or other harm to the individuals. The notification requirement applies only to health information that is “unsecured” – information that is not encrypted or destroyed and, therefore, is usable, readable, or decipherable by an unauthorized person. This approach not only will lead to more frequent reporting of breaches, but may also accelerate the movement toward encryption for electronic health systems. With Ontario’s Information and Privacy Commissioner frequently advocating the use of encryption so as to minimize potential breaches\(^\text{401}\), the move towards notifying of breaches involving unsecured information would appear to be consistent with current trends in Ontario’s health privacy climate.

The U.S. \textit{HITECH Act} demonstrates another trend that Ontario may, along with the other Canadian provinces and territories, may consider in addressing electronic health records – harmonized federal policy and legislation to which all provinces would adhere. This approach was suggested in Canada in the February 1999 report of the Advisory Council on Health Info-Structure, commissioned by the federal Minister of Health. The Council recommended that the federal Minister of Health should work with his provincial and territorial counterparts to improve patient care through the creation of provincial and territorial person-based, electronic health record systems. These systems would make accessible – on a need-to-know basis and under the control of patients – all relevant information about their past medical histories. The Council established several objectives for achieving these systems and proposed that the Minister of Health should “harmonize provincial and territorial privacy legislation to ensure that these

objectives are facilitated.\textsuperscript{402} These objectives included improving patient care, providing legislative safeguards against the use of identifiers, and improving the security of health records by exploiting modern technologies such as encryption.\textsuperscript{403} This view continued to be supported a few years later in the Romanow Report, which found that Canada Health Infoway should take the lead in promoting harmonized health privacy legislation across the country, and breaches of privacy should be treated as an offense under the \textit{Criminal Code of Canada}.

Prior to the \textit{HITECH Act}, the U.S. had enacted federal health privacy legislation, HIPAA, in an attempt to harmonize health privacy and security efforts across the country. HIPAA passed in 1996 with a focus on “portable” health insurance coverage that individuals could take from one employer to the next without having pre-existing health conditions acting as an impediment to job transitions. Another policy mandate of HIPAA was to move toward standardized electronic transactions for the health care industry, which brought concern about protected health information being put into electronic form. This concern led to the creation of the HIPAA Security Rule and the HIPAA Privacy Rule. The Security Rule specifies a series of administrative, technical, and physical security procedures for providers and plans to use to ensure the confidentiality of health information in electronic form. The Privacy Rule established several individual privacy rights with respect to such protected health information, including a right of access and the right to request that a covered entity restrict the use and disclosure of their protected health information for the purposes of treatment, payment, or other routine health care operations.\textsuperscript{404}

\begin{flushright}
\textsuperscript{402} Advisory Council on Health Infrastructure, “Paths to Better Health”, \textit{supra} note 17 at 3-10.\\
\textsuperscript{403} \textit{Ibid}.\\
\textsuperscript{404} 45 C.F.R. (2005), pts. 160, 164.
\end{flushright}
In February 2009, the U.S. government introduced the *American Recovery and Reinvestment Act* (i.e. the U.S. economic stimulus legislation), which included the *HITECH Act*. The *HITECH Act* includes three sets of provisions to promote health information technology (HIT) adoption: (1) the codification of the Office of the National Coordinator for Health Information Technology within the Department of Health and Human Services in order to facilitate the development and implementation of a strategic plan to guide the nationwide implementation of HIT in the public and private health care sectors; (2) financial incentives for HIT use among health care practitioners by establishing grant programs to provide funding for investing in HIT infrastructure, purchasing certified EHRs, training, and the dissemination of best practices; and (3) imposing new privacy and security requirements by amending and expanding HIPAA.

The changes to HIPAA include more aggressive enforcement of the HIPAA Privacy and Security Rules, including a substantial increase in civil penalties and the extension of new enforcement powers to the Department of Justice for the prosecution of criminal penalties and to state Attorneys General. *HITECH* also introduces periodic audits of organizations using EHRs by the Department of Health and Human Services in order to ensure compliance with the Privacy and Security Rules.

---

405 U.S. *HITECH Act*, *supra* note 1.
407 *Ibid.*, Subtitle D.
Similar to the approach of creating new, EHR-specific legislation in Ontario, a harmonized federal approach to regulating the privacy protections surrounding EHRs would enable legislators to consider Canadians’ definitions of health privacy and the values undermining privacy and to address the privacy problems that deserve legal protection in an electronic health environment. For example, a federal breach notification requirement would address concerns that arise when patient information travels across borders, such as in a recent situation when patient information got lost in transit from New Brunswick to British Columbia.\footnote{409}

This federal approach is also consistent with a recent article by Lawrence Gostin, in which he argued that bold federal regulations would be effective in safeguarding privacy, more uniform and fairer in application, and less likely to impede socially beneficial activities.\footnote{410} Although this is an approach that requires cooperation from other parties from outside of Ontario – such as Canada Health Infoway, federal and provincial Ministers of Health and federal and provincial information and privacy commissioners – it is worth mentioning here because of its potential to enable patients from across the country to experience the same controls over their personal health information and the same ability to limit access to this information, regardless of where they are in the country.


\footnote{410}{Lawrence O. Gostin, “Privacy: Rethinking Health Information Technology and Informed Consent” in Mary Crowley, ed., \textit{Connecting American Values with Health Reform} (Garrison, NY: The Hastings Center, 2009) 15 at 17, online: The Hastings Center \<http://www.thehastingscenter.org/uploadedFiles/Publications/Primers/privacy_gostin.pdf>.}
4.4 Determining the Best Legislative Route

Based on the analysis conducted on the three legislative options above, it is evident that while *PHIPA*, in its current form, addresses privacy in the three ways set out in the framework established in Chapter 3, it does not sufficiently contemplate the privacy problems associated with EHRs. *PHIPA* enables patients to control their personal health information by establishing strong consent and access frameworks, but it does not properly contemplate how these regimes would function in an electronic health environment. The Act does not sufficiently outline who has custody and control – and is therefore accountable for – personal health information collected by multiple custodians in shared electronic health record systems that function for the primary purpose of providing direct care to patients. Similarly, *PHIPA* enables patients to limit access to their selves through the lock box provisions, but it does not contemplate how this process will function in the EHR environment.

While *PHIPA* currently addresses several of the privacy problems identified in Chapter 3 as being worthy of legal protection, it does not sufficiently address how to protect against these problems in an electronic health environment. For example, *PHIPA* needs to provide stronger protection against surveillance through provisions on security safeguards and mandatory assessments, such as privacy impact assessments. *PHIPA* should also better address the possibilities for aggregation in the EHR, potential secondary uses of the EHR, and the specific challenges arising from identification and de-identification in EHRs. Finally, *PHIPA* should better contemplate problems associated with disclosure by addressing breaches of confidentiality and breach notification in an electronic health environment.

Despite being the most comprehensive health privacy legislation in Canada, *PHIPA* does not sufficiently contemplate a pan-provincial EHR that functions for the primary purpose of
providing direct care to patients. Therefore, legislators must consider the other options available to them for updating the legislative approach in Ontario. While the approach of introducing new legislation (Option #3) may have been suitable for the legislative schemes in B.C. and Newfoundland based on each province’s respective existing legislative regimes, it is important to keep in mind that neither of these provinces had health privacy legislation prior to introducing these pieces of legislation, while Ontario has already had success with PHIPA. As such, for Ontario to introduce an additional piece of legislation addressing health privacy may be an administratively burdensome approach and may cause unnecessary confusion in the provincial health care system with respect to compliance.

As demonstrated in Option #2 (section 4.2), several other Canadian provinces have amended and/or added regulations to their respective health privacy legislation in order to better accommodate for the privacy losses associated with EHRs. In order to update its health privacy scheme, this is the best approach for Ontario’s legislators and policymakers to take, in accordance with the legislative flexibility and requirements outlined in PHIPA. For example, PHIPA could include security safeguards that could improve against surveillance in EHR-specific regulations. This regulation could include general, technology-neutral provisions on access control, audit logging, identification, and authentication. Not only would this approach require health information custodians to take a uniform approach to implementing technical safeguards, but it could also provide guidance to organizations and vendors building EHR systems on what features to include in the technical design so that features such as audit logs and consent directives would be part of the system.

By amending PHIPA to include EHR-specific regulations, legislators would take a more proactive approach to regulating the protection of personal health information in an EHR
environment. This approach would enable patients to have greater control over their personal health information by directly incorporating consent and access requirements specific to EHRs into the legislation. Although this process has been recommended and is not likely to be an expeditious or simple, Ontario does not appear to have a better choice in ensuring that its legislation stays on pace with policy and technological developments for EHRs.

In order to work towards a coherent legal framework that appropriately protects the privacy and confidentiality of electronic health records, legislative attention surrounding PHIPA should focus on safeguarding patient privacy and ensuring confidentiality in an electronic health system. Patients will not trust EHRs unless their definitions of privacy are recognized; that is, they must be able to control their personal health information held in the EHR and to limit others’ access to this information. Of high significance, legislators must establish an accountability framework to determine the custodians in the EHR so that patients are able to know who is accountable for their information in the EHR. In order to recognize that privacy is a consent-based right, legislators must determine how a patient can properly consent in an EHR environment so that patients’ rights can be properly balanced with the benefits and risks associated with electronic health systems. This involves expanding the definition for implied consent to an EHR environment, ensuring that consent remains informed and knowledgeable, expanding lock-box to apply in the EHR context, and facilitating a method for patients to opt out of using the EHR. Although truly informed consent may be largely impossible to obtain from a patient regarding the uses and disclosures of her information in an EHR, PHIPA must mandate
informed consent for at least the initial collection of personal health information that will be added to the EHR.\textsuperscript{411}

This legal framework for EHRs must also protect the values of autonomy, dignity, and personhood, which are critical to privacy protections in an electronic health environment. If these values are properly protected in legislation and policy, several losses of privacy could occur that would potentially cause patients to not trust their personal health information in the EHR. As discussed above, this legislative framework should address privacy losses resulting from surveillance, aggregation, secondary use, identification, disclosure, and breach of confidentiality. This includes, for example, incorporating transparent and well-defined privacy safeguards, as have Manitoba’s and Alberta’s health privacy acts, which promote accountability by requiring data is used only for legitimate public purposes. Ontario legislators should build upon the current strengths of \textit{PHIPA} by enacting EHR-specific regulations that accommodate a legal framework that best protects patients’ values and definitions of privacy.

\footnote{\textsuperscript{411} For a further discussion of consent in the EHR context, see Ries, “Patient Privacy”, \textit{supra} note 71.}
Chapter 5
Conclusion

This paper has attempted to demonstrate that given the inadequacies of Ontario’s current health privacy legislation in addressing electronic health records, legislative and policy reform must take place so as to prepare Canada’s most populous province for the oncoming and ongoing proliferation of electronic records in the health care system. In working towards legislative reform, regulators must pay critical attention to reform measures taking place in other provinces in order to establish the best legislative route for Ontario. As I demonstrate in Option #1 in Chapter 4, it is clear that PHIPA cannot remain in its current form if the legislation is to stay consistent with and not serve as a barrier to Ontario’s successful implementation of a provincial EHR in the upcoming years.

In Canada, the development of EHR systems represents much more than the simple transformation of paper records in a family doctor’s office to electronic records that may be accessed, with appropriate controls, by Ontario health care providers, regardless of where they are in the province. Not only are EHRs modernizing and revolutionizing the management of information systems in the Canadian public health care system, EHRs also seem to be shifting the fundamental way in which an individual views his or her right to control the collection, use, transmission, and disclosure of his or her personal health information. In turn, the individual more strongly desires to limit who is able to access his or her personal health information and, ultimately, some of his or her most intimate and personal details. Given the active role that individuals are now able to play and will continue to play in the Canadian health care system, there is a strong need for regulators to understand the public’s views on EHRs and to gain public approval in the management of provincial EHR systems.
As such, the framework established in Chapter 3 sets out to capture the important role that privacy plays in public perception when it comes to legislating and managing the provincial EHR in Ontario. Regulators, politicians, and policymakers therefore need to understand the definitions and values of privacy associated with electronic health systems and the privacy losses that may result when these definitions and values of privacy are not properly addressed.

In applying the framework for privacy in an electronic health environment to three legislative and policy options in Chapter 4, it seems most reasonable and advantageous to Ontario to proceed with Option #2, which involves amending PHIPA to include EHR-specific regulations that better contemplate for both primary and secondary uses of EHRs in Ontario. As recommended by the Standing Committee for Social Policy in its mandated three-year review of PHIPA, the legislation should be updated to allow the development of a more comprehensive range of regulations related to e-health with a view to accelerating e-health initiatives. The fact that legislation enacted only five years ago can already become outdated demonstrates the pace with which EHRs are being and need to be implemented in Ontario and in Canada.

In developing legislative changes to the health privacy framework in Ontario, legislators and policymakers should work together to accommodate accelerating e-health development. They must realize how Ontarians define their right to privacy in an electronic health environment and what fundamental values undermine these definitions. Further, they must use these definitions in order to identify the privacy problems that are worthy of protection in an electronic health environment. Finally, they must realize that the failure to properly address the privacy problems requiring this protection may lead to various privacy losses associated with personal health information and to the loss of public confidence in EHR systems. By taking a flexible approach to considering the definitions, values, and problems of privacy set out in the framework
in Chapter 3, regulators could overcome one of the difficulties associated with developing proper privacy protections in an electronic health environment, namely that a broad and diverse range of privacy rights is taken into consideration and that these rights are properly balanced against one another.

In looking at a range of options for regulating the electronic health environment in Ontario, I have attempted to demonstrate that legal and policy ideals must be considered in the early stages of technological innovation and legislative reform. Undoubtedly, further public debate is needed to understand how these ideals will influence how Ontarians manage their health care.