# Practices for protecting privacy in health research: Perspectives of the public, privacy guidance documents and research ethics boards (REBs)

Mary Lysyk

Thesis submitted to the Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for
the PhD degree in Population Health

Population Health PhD Program
University of Ottawa

ABSTRACT

Health research is the single vehicle for uncovering the varying causes of disease or illness, understanding the broader determinants of health, and discovering new or to validating traditional ways of treating the individuals who suffer from these conditions [5-7]. Thus, health research activities are at the heart of medical, health and scientific developments [8].

While health research activities exemplify some of the greatest hopes for improved health-care, they also highlight public concerns for the protection of personal health information (PHI) [6;7;9-11]. More specifically, advances in modern information technology and the increasing pace of international collaborative studies raise challenging issues regarding privacy protection in health research [12;13]. The extensive quantities of data housed in general-use databases and electronic health records (EHRs) are two frequently cited examples of "electronic health information" that are now increasingly available to researchers globally (p. 233) [3]. For example, individual discrete studies are expanding into long-term prospective disease or treatment databases without clear research questions and involving multiple research teams and jurisdictions [3;14-16]. As well, EHRs are increasingly taking a prominent role in Western industrialized nations such as England, Australia, New Zealand, Germany, the Netherlands, the United States, as well as Canada [17]. The expected large scale demand for the secondary uses of personal health information (PHI) from electronic health records represents another significant challenge to privacy [15;16]. EHRs facilitate clinical and population-based health research not only in terms of secondary uses, such as retrospective observational studies, but also for prospective cohort studies [15;16].

In Canada today, there are two documents that provide direction that is applicable at a national level to privacy protection practices in health research: *The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2*) and the *CIHR Best Practices for Protecting Privacy in Health Research* (CIHR BPPP). The TCPS 2, a policy document, is the most influential Canadian policy applicable to the ethics of research with human participants and widely followed by Canadian researchers and institutions.

Conversely, use of the CIHR BPPP is purely optional. Canadian REBs are responsible for much of the governance of privacy, confidentiality and security in health research. However, the extent to which they apply and utilize the privacy provisions from the TCPS 2 and CIHR BPPP in their protocol requirements is not known.

This thesis provides a descriptive comparative study of the international and Canadian contexts for privacy protection in health research and produces a greater understanding of two Canadian stakeholder groups: the Canadian public, whose participation and trust is imperative for valid research; and Canadian Faculty of Medicine (FoM) university biomedical REBs with whom much responsibility for ensuring appropriate protection of privacy and confidentiality in health research rests.

## TABLE OF CONTENTS

**Page**

## LIST OF ACRONYMS

**AAPOR:** American Association for Public Opinion Research

C**IHR BPPP:** Canadian Institutes of Health Research Best Practices for Protecting Privacy

**CIOMS:** Council for International Organizations of Medical Research

**CSA:** Canadian Standards Association

**EHI**: electronic health information

**EHR**: electronic health record system

**EU**: European Union

**FIPs**: fair information principles

**FoM REB**: faculty of medicine university research ethics board

**HIPAA**: (Unites States) *Health Insurance Portability and Accountability Act*

**OECD:** Organization for Economic Cooperation and Development

**PHI**: personal health information

**QUOROM**: Quality of Reporting of Meta-analyses

**REB**: research ethics board

**TCPS 2**: Tri-Council Policy Statement on Ethics of Research Involving Humans, Second Edition

**UNICEF**: United Nations Children's Fund (formerly United Nations International Children's Emergency Fund)

**UN**: United Nations

**UK**: United Kingdom

**US**: United States

**WMA**: World Medical Association

## GLOSSARY OF TERMS

**Confidentiality**: "an ethical and/or legal responsibility of individuals or organizations to safeguard information entrusted to them, from unauthorized access, use, disclosure, modification, loss or theft." [1]p. 190.

**Consent**: "an indication of agreement by an individual to become a participant in a research project. Throughout this Policy, the term "consent" means "free (also referred to as voluntary), informed and ongoing consent." [1]p.190.

**Data**: records or observations in digital form that stand for observed values or actions [2].

**Database(s)**: digital, ordered collections of data that have varying purposes. Collections can serve highly specialized purposes or be a resource for changing multiplicity of uses. They can be longitudinal in nature or one-time collections. As well, they vary in size from small to extensive. In research, almost all data collections are now stored and handled as digital databases [2].

**Electronic health information (EHI):** personal health information (see PHI below) contained in either databases or electronic health records [3].

**Electronic health record systems (EHRs)**: comprehensive, interoperable, digital patient record systems that, due to their very nature of interconnectedness, can be used beyond direct patient care for healthcare service evaluation, public health purposes and health research [2].

**Full research ethics board (REB) review**: "the level of REB review assigned to above minimal risk research projects. Conducted by the full membership of the research ethics board, it is the default requirement for the ethics review of research involving humans."[1] p.192.

**Research ethics board (REB)**: "a body of researchers, community members, and others with specific expertise, e.g., in ethics, in relevant research disciplines, established by an institution to review the ethical acceptability of all research involving humans conducted within the institution's jurisdiction or under its auspices."[1] p.196.

**Secondary use of data**: the use of data that already exists for a purpose different from the one originally declared. For this thesis, secondary use will refer specifically to data obtained from either paper or electronic health record systems (EHRs) for primary healthcare and used for health research purposes [2;4].

**Personal health information (PHI)**: health or health-related information that may reasonably be expected to identify an individual, alone or in combination with other available information. This is further classified as:

- **Directly identifying information** – "the information identifies a specific individual through direct identifiers, e.g., name, social insurance number, personal health number." [1] p.193.

- **Indirectly identifying information** – "the information can reasonably be expected to identify an individual through a combination of indirect identifiers, e.g., date of birth, place of residence, or unique personal characteristic." [1] p.193.

- **Coded information** – "direct identifiers are removed from the information and replaced with a code. Depending on access to the code, it may be possible to re-identify specific participants, e.g., the principal investigator retains a list that links the participants' code names with their actual names, so data can be re-linked if necessary. [1] p.193.

- **Anonymized information** – "the information is irrevocably stripped of direct identifiers; a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining indirect identifiers is low or very low." [1] p.193.

- **Anonymous information** – "the information never had identifiers associated with it, e.g., anonymous surveys, and risk of identification of individuals is low or very low." [1] p.193.

**Privacy**: in this thesis, privacy will be referred to in terms of information privacy. Information privacy is defined as the right of individuals to determine when, how and to what extent they share information about themselves with others [4].

**Privacy risks**: "the potential harms that participants, or the groups to which they belong, may experience from the collection, use, and disclosure of personal information for research purposes." [1] p.195.

**Prospective broad-use database**: the thesis defines this concept as a non-mandatory collection from a cohort, i.e., no authority exists in legislation for the collection, use and disclosure of PHI, and for which one cannot articulate a clear research question or all the intended uses of the data [3].

**Security**: "measures taken to protect information. It includes physical, administrative, and technical safeguards" [1] p.196.

## REFERENCES


(1) Tri-Council Policy Statement: Ethical Conduct of Research Involving Humans - Second Edition, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (2012).

(2) Lowrance, WW. *Privacy, confidentiality and health research*. Cambridge: Cambridge University Press; 2012.

(3) Willison D, Gibson E, McGrail K. **A Roadmap to Research Uses of Electronic Health Information.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011.

(4) Canadian asqwZs of Health Research. CIHR Best Practices for Protecting Privacy in Health Research. Ottawa: Public Works and Government Services Canada; 2005. Date accessed 20/05/2006. www.cihr-irsc.gc.ca/e/29072.html

## LIST OF FIGURES

**Page**

## LIST OF TABLES

**Page**

CHAPTER 3



CHAPTER 4



CHAPTER 5

CHAPTER 6

## ACKNOWLEDGMENTS

*"Look at every path closely and deliberately. Then ask yourself alone, one question. Does this path have a heart? If it does, the path is good."* – Carlos Castaneda

This is a question I have asked myself many times throughout this dissertation. And I am very fortunate and grateful to say that I always found the "heart" during this challenging path. This largely came from the love of learning and perseverance that my parents, Dmytro and Paraskevia Lysyk, instilled in me. And through the many people who have stood by me and supported me along the way.

Ian Graham is a supervisor of superb insight, tremendous patience and is a model of good scholarship. I am grateful for his ability to keep me focused and on track, particularly during the roughest and toughest parts of this journey. My sincerest thank you.

To my examination committee, Professor Mary Egan (University of Ottawa), Dr. Ray Saginur (Ottawa Hospital Research Institute), Mr. Ross Hodgins (formerly of the Information Commissioner of Canada) and Professor Yann Joly (McGill University). I am very appreciative to all for your valuable input and suggestions which only helped strengthen and improve this research. Thank you for your comments.

To my friends and colleagues, Sandra Chatterton, Susan Fox and Marylea Cameron Reid. You are all strong women who inspired me and kept me going during the different phases of this work. You have been amazing friends. Thank you for being there.

To my past and present colleagues at Health Canada. This work could not have been completed without the resources and "in-kind" contribution of the Program. Your support and encouragement made this possible. And a special thank you to Pat Milliken who has been a privacy policy mentor to me and yet another example of strength and inspiration.

I would also like to thank Ms. Roseline Savage from the Population Health PhD program who has been so kind and helpful since the beginning of the Program.

And to my family. John, you always believed in me and especially when I did not. You stood solidly by me and kept me going. This degree is as much yours as it is mine. But most of all you supported me in making sure our beautiful daughter Rachel always came first. And she always will.

This work is dedicated to the memory of my father. He is an example to me and everyone who knew him of quiet strength, integrity, a warm smile and tremendous perseverance against all odds. He is with me always.

# CHAPTER 1:
# INTRODUCTION AND BACKGROUND

## Introduction

Health research is the single vehicle for uncovering the varying causes of disease or illness, understanding the broader determinants of health, and discovering new or to validating traditional ways of treating the individuals who suffer from these conditions [5-7]. Thus, health research activities are at the heart of medical, health and scientific developments [8].

While health research activities exemplify some of the greatest hopes for improved health-care, they also highlight public concerns for the protection of personal health information (PHI) [6;7;9-11]. More specifically, advances in modern information technology and the increasing pace of international collaborative studies raise challenging issues regarding privacy protection in health research [12;13]. The extensive quantities of data housed in general-use databases and electronic health records (EHRs) are two frequently cited examples of "electronic health information" that are now increasingly available to researchers globally (p. 233) [3]. For example, individual discrete studies are expanding into long-term prospective disease or treatment databases without clear research questions and involving multiple research teams and jurisdictions [3;14-16]. As well, EHRs are increasingly taking a prominent role in Western industrialized nations such as England, Australia, New Zealand, Germany, the Netherlands, the United States, as well as Canada [17]. The expected large scale demand for the secondary uses of personal health information (PHI) from electronic health records represents another significant challenge to privacy [15;16]. EHRs facilitate clinical and population-based health research not only in terms of secondary uses, such as retrospective observational studies, but also for prospective cohort studies [15;16].

Both data access and privacy, confidentiality and security issues raised by advancing technologies are more challenging today than ever before [3;12]. What is particularly noteworthy is that new privacy issues and concerns are shared by many Western

industrialized countries and extend well beyond health research [3;12]. This is not only due the increasing pace of international collaborative exchanges of personal information but also global efforts at harmonizing privacy, confidentiality and security standards [3;12].

## Challenges to privacy

In his germinal book, *Privacy, Confidentiality and Health Research*, William Lowrence highlights the importance of protecting privacy and maintaining confidentiality of PHI if the full potential of modern technologies and electronic health information is to be realized in health research [2]. More specifically, he repeatedly indicates that the issue is one of trust, and that determinants of trust and trustworthiness are important in understanding whether individuals will release sensitive personal information in health research [2]. Wavering trust will translate, at least in part, to reduced participation by the public in health research [19-21]. Furthermore, numerous studies consistently show that eligible research participants often refuse to give consent to participate in health research, even if PHI will be de-identified [19-21]. Low participation will bias and even jeopardize research data quality and generalizability [19-22]. This speaks to the importance of maintaining appropriate privacy, confidentiality and security safeguards for identifiable and de-identified PHI.

In addition, studies have questioned if Canadian research ethics boards (REBs) have the expertise needed to assess privacy and compliance with legislative and policy requirements in research protocols [23;24]. This can result in inconsistent REB decisions across the country, making it difficult for researchers to know which practices to follow in terms of ensuring the privacy, confidentiality and security of PHI entrusted to them [23;24].

Public opinion surveys and focus groups demonstrate that the public expects researchers, research institutes, government and private research organizations to act in responsible, ethical and accountable ways regarding both the identifiable and de-identified data entrusted to them [25;26]. From the public's perspective, safeguards, checks and balances must be in place to ensure that this happens [25].

Internationally, many countries such as the UK, US, Australia, and health organizations including WHO, UNESCO and CIOMS, provide privacy guidance for health research [27-37]. Some documents such as the *Declaration of Helsinki* , *Ethical Guidelines for Biomedical Research Involving Human Subjects* and the *ICH Good Clinical Practice: Consolidated Guidance*, though not specific to privacy, are considered gold standards in ethics by the international health research community [7]. While studies have compared privacy legislative requirements globally, to the author's knowledge, none have examined the concrete application of these requirements by conducting an item-by-item privacy practice comparison. Therefore, how Canadian documents measure-up to similar international documents is not known.

In Canada today, there are two documents that provide direction that is applicable at a national level to privacy protection practices in health research: *The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2*) and the *CIHR Best Practices for Protecting Privacy in Health Research* (CIHR BPPP). The TCPS 2, a policy document, is the most influential Canadian policy applicable to the ethics of research with human participants and widely followed by Canadian researchers and institutions. Conversely, use of the CIHR BPPP is purely optional. Canadian REBs are responsible for much of the governance of privacy, confidentiality and security in health research. However, the extent to which they apply and utilize the privacy provisions from the TCPS 2 and CIHR BPPP in their protocol requirements is not known.

This thesis provides a descriptive comparative study of the international and Canadian contexts for privacy protection in health research and produces a greater understanding of two Canadian stakeholder groups: the Canadian public, whose participation and trust is imperative for valid research; and Canadian Faculty of Medicine (FoM) university biomedical REBs with whom much responsibility for ensuring appropriate protection of privacy and confidentiality in health research rests.

## Purpose and Objectives

One of the aims of this work is to gain an understanding of the Canadian public's views about privacy, confidentiality, and security practices (regarding PHI protection) in light of advancing technologies. EHRs and their secondary uses for health research purposes will therefore be emphasized when examining the public's perceptions.

Additionally, research outcomes will identify the provisions the international health research community recommends for protecting PHI (in terms of privacy, confidentiality and security practices) in general and with regards to the creation of broad-use databases and secondary uses specifically, and how these provisions compare to the Canadian context.

How Canadian FoM REBs ensure that PHI is protected, to the author's knowledge, has never been explored. FoM REB website research protocol requirements will be examined to gain an understanding of how they apply and utilize Canadian privacy guidance and policy documents.

Finally, any new and innovative privacy protection practices that are being utilized to address current privacy risks and challenges both internationally and locally will be identified and discussed.

In order to address the above, the thesis has three specific objectives:

1) To identify a trust/risk privacy theoretical framework that will serve as a model for analyzing and predicting health research participants' privacy, confidentiality and security concerns and that will be applied to a systematic review of public opinion surveys focused on EHRs and the secondary uses of PHI.

2) To conduct a descriptive comparative analysis of international privacy best practices using the TCPS 2 and CIHR BPPP (with a particular focus on prospective broad-use databases and secondary uses of data). This will provide an understand of how international standards vary

in their handling of privacy, confidentiality and information security issues, how the Canadian documents compare, as well identify innovative or "new" practices; and

3) To identify and list Canadian FoM REBs' research protocol requirements (as indicated on their website policy and application documents and with a particular focus on prospective broad-use databases and secondary uses of data) for ensuring appropriate protection of privacy, confidentiality and security of PHI in health research.

**Thesis rationale**

This thesis has important implications for health research and in particular population health practice and policy. For example, prospective broad-use databases and interoperable EHR systems have the potential of cumulating lifetime personal health information about an individual, including the broader determinants of health, e.g., socio-economic conditions, education, culture, gender, that would be invaluable for population health research [17;38]. The results of this thesis expand the current knowledge base regarding the processes involved in research participants' trust and willingness to provide their PHI data for health research purposes. Understanding the complex variables and relationships (through a trust-risk model) will ensure optimal strategies and mechanisms to enhance participant-researcher trust as much as possible.

Secondly, the international document analysis of privacy practices provides new information on how the Canadian documents compare to global privacy practices in health research.

Finally, the last paper in this thesis is fundamental, both conceptually and methodologically to understand FoM REB requirements for protecting PHI. It highlights how privacy policy and guidance documents, specifically the TCPS 2 and CIHR BPPP, have been applied by FoM REBs as well as the differences and commonalties that exist across FoM REBs. Providing a list of "new" or "innovative practices" demonstrates how REBs are attempting to address emerging issues. By including privacy protection for both paper and electronically stored data, a comprehensive review of privacy protection practices is provided. To the author's knowledge, this is the first time such an analysis has been conducted.

Findings from this study can be applied to this multi-jurisdictional issue both horizontally, i.e., across FoM REBs, as well as vertically, i.e., provincially and federally including Tri-council agencies, in order to facilitate harmonization and standardization of privacy policies and practices that build meaningful public trust that PHI is protected in health research.

## Background and summary of literature review

### *The increasing role of EHRs and prospective databases in health research*

The increasing role of EHRs in shaping the Canadian health-care landscape is well recognized [39-41]. The EHR is emerging as the key information and communications foundation for our health-care system [39-41]. Due to the potential for interoperability and instantaneous access, EHRs have the capability to improve the quality of health-care delivery, reduce costs and facilitate health services planning and research [39-41].

In Canada, EHR systems are emerging in varying stages and with different components within jurisdictions across the country [42]. Examples from both clinical and research contexts include the development of clinical registries and networks for pharmaceutical, laboratory and diagnostic imaging information [42]. As Canadian health-care moves towards the integrated use of EHRs in direct patient care, the health research community is seeing a proliferation of database research as well as the development of prospective broad-use databases [3]. In the case of broad-use databases where the data comes from clinical practice, EHR is *the* electronic data collection system [23].

There are numerous clinical and research benefits to EHRs, however significant barriers to its use also exist. The Kirby Senate Report on health-care states:

> "Currently, there are three main privacy issues that must be addressed for EHRs to become a reality in Canada in the next five to seven years. These are:
>
> 1. The need for a more harmonized approach to privacy across all jurisdictions to allow for more consistent conditions for sharing personal health information among users and more consistent protection of personal health information for patients.
>
> 2. The need to develop robust and effective privacy safeguards, policies and procedures that can be implemented in a pragmatic, practical and cost-effective manner.
>
> 3. The need to build public confidence that personal health information will be protected in an electronic world" p. 181 [41]..

Professor Elaine Gibson, Faculty of Law, Dalhousie University, reframes the concept of personal information protection not as a barrier to EHR implementation, but rather as an essential component of an EHR infrastructure that is essential to maintaining Canadians' trust

and ensuring that their PHI is receiving the highest level of protection [43]. The results of numerous public opinion surveys of Canadians lends credence to Professor Gibson's position, both for primary health-care and for health research [26;44-46]. EHRs create a risk to privacy that is more extensive and harder to manage than when working with paper-based records alone [47]. If trust in the EHR is eroded, what are the consequences to primary care and health research? The answer to this question remains unclear.

While the EHR is still in the early stages of rollout, prospective broad-use databases are proliferating [3;14]. Firstly, a distinction must be drawn between prospective broad-use databases where participation is not mandatory, and mandatory public health clinical registries. Participation in non-mandatory collections of PHI are typically consent-based and subjects can usually withdraw at any time when the collection has direct identifiers [1;3]. As well, REB approval is required prior to the start of data collection [1;3]. Conversely, mandatory public health registries have authority to collect PHI not in consent models but rather through legislative authority, e.g., communicable diseases registries and the British Columbia's *E-Health Act*, and, as such, have standards that are not applicable to other prospective collections [1;48]. The privacy protection requirements of non-mandatory collections of PHI in broad-use databases have been subject to few empirical studies and as such, little is known about the privacy requirements and management of confidentiality in these contexts [3;14;49]. When examining prospective broad-use databases, this thesis will exclusively focus on those that are non-mandatory collections and subject to REB approval.

## Overview: Canadian privacy legislation

Understanding Canadian privacy statutes, frameworks and guidelines as they relate to health research is a critical first step in framing the complexities of personal health information and health research in the Canadian context. A review of privacy legislation and practice standards is therefore provided below.

The Canadian privacy legislative landscape is a patchwork, and numerous organizations and institutions have expressed concerns about the challenges of complying with overlapping or even conflicting legislations [42]. For example, in terms of protecting personal health

information, Canadian jurisdictions often apply different rules. Public sector legislation (which is typically found as a section in access to government information legislation), varies considerably across the country both in terms of provisions and application. For instance, some jurisdictions include institutions such as hospitals, universities and regional health authorities, while other jurisdictions do not. Conversely, the core federal legislative provisions and constitutional documents focusing on protecting privacy, confidentiality and security of personal health information include the Canadian Charter of Rights and Freedoms, the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Privacy Act [50;51;52].

Private sector legislation is governed by the 10 principles in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information. The CSA 10 principles were codified into law through the Personal Information Protection and Electronic Documents Act (PIPEDA) [52], which was implemented in a staged approach between 2001 and 2004. PIPEDA governs how the private sector (including private clinical and physician practices) collect, use, disclose and dispose of personal information [53]. In terms of personal health information specifically, legislation governing health information privacy and management has been enacted by many provinces within the past few years. This legislation spans both the public and private sectors. **Figure 1-1** provides an overview of the complexity of the Canadian privacy landscape today.

# Figure 1-1: Overview of Privacy Legislation in Canada and Oversight Bodies


Current to September 1, 2013
Source: Office of the Privacy Commissioner of Canada, Fact Sheets Privacy Legislation in Canada, http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp.
Accessed September 1, 2013

In summary, the proclamations of numerous Canadian personal health information laws over the past decade, and in particular, the past few years have led to much uncertainty and confusion on the part of the health research community [3]. Researchers and research ethics boards have expressed concern about interpretation of the relevant laws, policies and guidance documents [3]. Lack of consistency in the legislation is yet another factor that has been raised in the literature, particularly given the cross-jurisdictional nature of many research studies being conducted today [3]. This results in further confusion and frustration on the part of health researchers [3]. Some have gone so far as to express the concern that all of the complexities of the new legislation will make conducting some types of cross-jurisdictional research impossible [3]. As a result, there has been a call for instituting standards and guidelines to clarify privacy legislation [3;54;55].

## Implications for population health practice and health policy

Negative perceptions of personal data privacy by the public can reduce trust and participation in health research [23].

Understanding the public's perception about privacy in the health-care context in general and regarding health research specifically is particularly important given advancing technologies [10]. Determining whether the systems the health research community has in place to engender public trust are adequate is timely and highly relevant to policy-makers [47] . Outcomes from this study can be used to develop more systematic approaches to protecting privacy in population health research; to audit information use practices and safeguards; to establish and strengthen reporting relationships to the Information/Privacy Commissioner; and thus meet the Canadian public's expectations that concrete steps are being taken to protect personal health information privacy, security and confidentiality in health research contexts [10;15;16;25;49;56;57].

Specifically, the findings from this work can be applied to general health policy and population health practice in the following ways:

- To assist in the development of a proportional model (scaling protections to appraised privacy risks) in health research using privacy practices emerging from the research outcomes;
- Additional privacy practices from international documents: REBs can be emulated or avoided in future revision of the TCPS or CIHR BPPP documents;
- To inform the establishment of standards to assist REBs in evaluating protocols that use PHI, and promote consistency across the country;
- To aid population health researchers in implementing appropriate privacy, confidentiality and security safeguards;
- To establish a baseline mechanism that can be used for auditing members of the health research community including researchers, research organizations, institutions and facilities as well as REBs' minimum standards regarding the privacy, confidentiality and security of personal health information;

## Thesis Format and Dissertation

The thesis format consists of a guiding privacy theoretical framework and three original articles. The privacy theoretical framework is presented in **Chapter 2**, and is based on public trust and risk beliefs (and the variables that influence them) in determining whether an individual will choose to participate and provide their PHI data in health research.

The first manuscript is presented in **Chapter 3**. It is a systematic review spanning ten years of public opinion research focused on the Canadian public's perceptions about their health information privacy in general, and related to health research specifically. This paper relates strongly to the framework as it examines perceptions about privacy protection in the dimensions of collection, control, transparency/awareness, unauthorized access, and the secondary uses of PHI, in order to better understand these variables and the roles they play in building public trust and managing risk beliefs.

In **Chapter 4**, the second manuscript begins with a review and analysis of fair information principles (FIPs) and their role in developing privacy legislation and guidelines. The chapter also introduces the list of items derived from the CIHR BPPP, TCPS 2 and international best practices. It also includes how Canadian documents compare to the international guidance documents; it identifies what additional elements are currently used in different countries to protect PHI in health research (and that are not included in the TCPS 2 and/or CIHR BPPP documents) and how these compare with FIPs.

In **Chapter 5**, the third manuscript discusses and investigates how, for the first time, a formal protocol is used to identify the privacy practices required by Canadian FoM REBs and how these practices compare to those outlined in the TCPS 2 and CIHR BPPP documents. As well, additional practices not found in either the TCPS 2 or CIHR BPPP are identified and discussed.

**Chapter 6**, the last chapter, provides an integration of study findings from two perspectives: developing a revised Trust-Risk Privacy Theoretical Framework and a discussion of harmonization and standardization of practices to protect PHI as a way forward.

The three articles that emerged from this thesis are being prepared for publication in scholarly journals such as Canadian Medical Association Journal, Electronic Healthcare, Canadian Health Services and Policy Journal, and the Journal of Medical Internet Research.

There are few ethical concerns associated with this work, considering the study design and the nature of the documents. This study exclusively uses documents that are available in the public domain or with express written consent from the authors if required (in the case of some syndicated public opinion research studies). Expedited research ethics approval was sought and received on November 24, 2008.

All elements of the work were conducted in conformity with the rules and regulations of the Faculty of Graduate and Postdoctoral Studies of the University of Ottawa and the Population Health PhD Program.

# CHAPTER 2:
# CONCEPTUAL FRAMEWORK

## Organizational ethics in health research

Health research organizations such as universities, hospitals, research institutes, government research organizations and private research firms all share the concept of organizational ethics. The definition the thesis utilizes for organizational ethics is as follows: "Simply expressed, *organizational ethics* is the study and practice of the ethical behaviour of organizations. It involves clarifying and evaluating the values embedded in organizational policies and practices, and seeking mechanisms for establishing morally acceptable values-based practices and policies" [58] p.33.

Organizational ethics is an emerging field in applied ethics that brings together two distinct and well-developed bodies of literature: *bioethics* and *business ethics* [58]. In Canada, while for-profit research organizations exist, a considerable amount of health research takes place through universities or health-care facilities such as hospitals or government facilities. While these organizations are not-for-profit and often thought of as "social institutions", they are also businesses [58]. From utilizing vision and mission statements, to balancing budgets, maintaining physical and human resources, seeking funding grants, and incorporating accountability structures such as a Board of Directors, and complying with applicable legislations, business-model elements figure prominently in these organizations [58]. As well, many ethical dilemmas now facing health-care and health research facilities are also present in *business ethics* [58]. It is well documented that privacy of personal information in electronic environments is an excellent example of an issue that straddles both the business and health-care (including health research) spheres [26;56;59-64]. Business ethics emphasizes the importance of learning from business models, conducting stakeholder analysis, developing proactive risk assessment and management strategies and promoting corporate and collective responsibility.

Additionally, *bioethics* or "medical ethics" provides three key contributions: it underscores responsibilities to individual patients or clients; it contributes tools such as professional codes of conduct; and it highlights the interests and well-being of patients/clients [58]. Bioethics

emphasises that researchers have a responsibility to each individual participant to protect their personal health information privacy and well-being more generally.

*Organizational ethics* shifts focus away from reacting to ethical problems as they arise, towards preventing ethical problems through various organizational strategies [58]. Privacy has been identified as one of the most important ethical issues of e-commerce and contemporary management practice [65]. Towards this end, examining the empirically tested business models that focus on the public's concerns related to releasing personal information in an e-commerce context is an important first step according to an *organizational ethics* approach.

## Conceptual model from e-commerce information: analysing and predicting consumers' privacy concerns when buying products or services online

In the private sector, research focuses on understanding and predicting consumer reactions to requests for personal information in electronic environments, e.g., e-commerce [56;63;64;66]. Researchers conceptualize that a long-term exchange of information privacy is initiated when a consumer releases personal information to a marketer [56]. Research in this area concentrates on understanding how consumers determine when they will engage in this long-term relationship, consumers' privacy concerns when releasing personal information online, as well as predicting consumer reactions to requests for personal information [56]. Understanding consumers' decisions to release or not release personal information is also central for the health research community [23;24;67;68].

A number of preliminary studies have shown that organizational practices, individuals' perceptions of these practices and the consequential societal responses are inextricably linked in many ways [63]. Causal models and theories are emerging from the e-commerce literature that explain these linkages, specifically their relationship to organizational information privacy practices in e-commerce [63]. The e-commerce model is comprised of three core theories: social contract theory (SC) [56], the trust and risk beliefs model [56;69;70], and the theory of reasoned action paradigm (TRA) [56;66;71].

Malahorta et al (2004) [56] validated the causal model focused on consumers' information privacy concerns in an e-commerce context and related to releasing personal information when individuals buy products or services online. As the only empirically verified model that directly relates to trust and risk beliefs, a version customized by the author for the health research context serves as a foundation for the three thesis manuscripts.

## Proposed trust-risk privacy theoretical framework for analysing and predicting health research participants' concerns for information privacy

The proposed privacy Trust-Risk Theoretical Framework is presented in **Figure 1**. While not validated in either the e-health or health research contexts, it was developed for the purpose

of this thesis by drawing on the proven theories and paradigms as described in e-commerce [25]. The model will be described in terms of both primary and secondary uses of data from EHR environments.

***Social Contract Theory (SC)***

SC theory has been used to explain behaviour in the context of information privacy [72;73]. A key principle of SC theory is an equitable exchange and shared understanding about contractual terms and self-control over the course of a relationship [56;72;73]. In the context of information privacy, SC theory suggests that an organization's *collection* (equitable information exchange) of personal information is perceived to be fair only when the individual providing personal information is granted *control* (consenting to opt-in or the choice to opt-out). Furthermore, the individual should be informed about the organization's intended use of the personal information and there is thus a *transparency and awareness factor* (openness and awareness about established conditions and practices) [56;72-77].

The three major dimensions emerging from SC theory, collection, control, and awareness of privacy practices, empirically show online consumers' concerns about information privacy [56]. In the healthcare and health research contexts, awareness is now reframed as the public's need for greater transparency of information that could increase the public's understanding about privacy practices[25]. Two additional dimensions are identified in the scientific literature that increase an individual's trust about organizational privacy, confidentiality and security practices: *preventing unauthorized access* and the *authorization for secondary uses* of the data [25]. For the purposes of the thesis, secondary uses will refer exclusively to uses of data from primary healthcare data collections to support health research initiatives.

A citizens' dialogue conducted in 2007confirmed that a system of checks and balances will allow the public to have confidence and trust in how PHI is managed in the health research context [25]. Both policy and guidance documents are therefore cast as having a positive impact on the dimensions of SC theory. Consistent with the e-commerce framework,

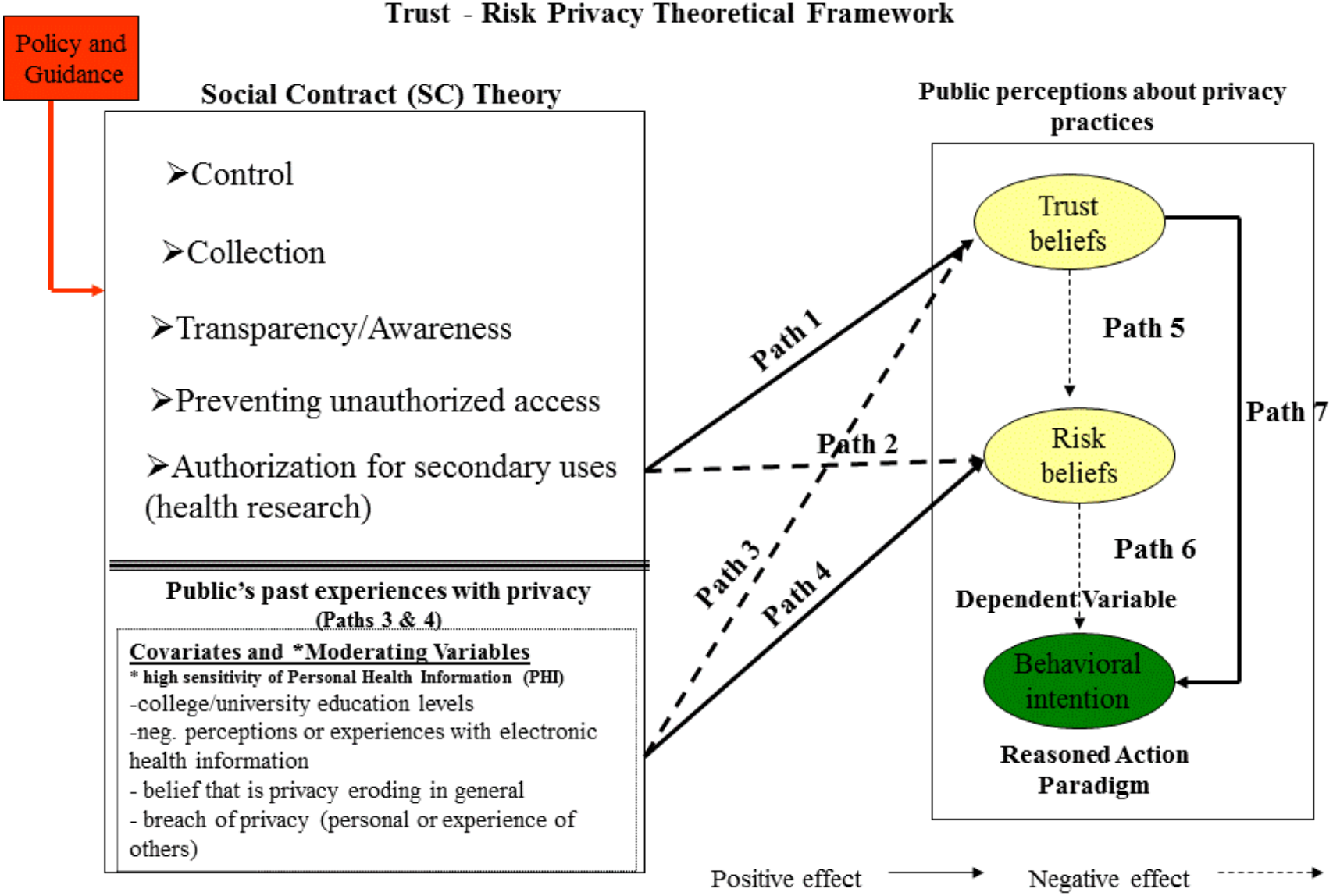
positive impacts on the SC dimensions build research participant trust **(Figure 2-1, Path 1)** and decrease risk beliefs **(Figure 2-1, Path 2)**.

***Covariates and moderating variables***

Several studies have shown that higher education levels, negative online experiences, perceptions of privacy erosion and invasion of privacy experiences are all found to negatively impact trust beliefs and increase risk beliefs [78;79]. As a result, they are included in the privacy theoretical framework but reframed to fit the e-health and health research context. While they will not be directly discussed in this work, their hypothesized positive impact on trust/risk is illustrated in **Figure 2-1**, **Paths 3-4**.

## Figure 2-1

**Trust - Risk Privacy Theoretical Framework**



In addition, the type and sensitivity of information being requested has shown to directly moderate risk beliefs for online consumers [56;80;81]. Specifically, more sensitive information is viewed by consumers as a higher risk to release than less sensitive information [56;73]. Financial and health information are ranked as the most sensitive of personal information [26;44;81]. This relationship is also reflected in **Figure 2-1, Paths 3-4.**

***Trust beliefs, risk beliefs and intention***

The trust/risk-intention model is used by researchers studying the for-profit private sector to explain client behaviours in uncertain commercial environments including client-firm relationships [82]. The model states that in situations when potential risks are present or perceived, trust plays an important role in predicting an individual's behaviour [83;84]. There is a substantive body of research showing that trust and risk are the two most significant beliefs where information privacy is involved in e-commerce [81;85;86].

Trust beliefs refer to the degree to which individuals believe that an organization is dependable to protect their personal information [87]. Risk beliefs refer to the high possibility for loss associated with release of personal information to the organization [88]. The research demonstrates that enhancing trusting beliefs will have a negative effect on risk beliefs (reduce risk perceptions) and finally facilitate intention to release personal information [56]. In the Privacy Framework, these relationships are reflected in **Figure 2-1, Paths 5-6.**

### *Reasoned Action Paradigm*

The Reasoned Action Paradigm states that behaviour intention is a reliable predictor of actual behaviour [66;71]. Malhotra et al [56] show that in the context of online e-commerce, trusting beliefs have a direct positive effect on the intention to reveal personal information. This relationship is reflected by **Figure 2-1**, **Path 7**. The Reasoned Action Paradigm therefore provides the conceptual missing link between understanding an individual's trust/risk beliefs and whether they opt to participate and release their accurate personal information to healthcare providers and health researchers.

## Summary

Organizational ethics highlight the application of both business models and stakeholder analyses to healthcare and health research organizations. Stakeholder analysis is crucial to identifying key interests and concerns that are needed in shaping organizational policy decisions and practices [58]. A significant stakeholder is the Canadian public, whose personal health information is requested either directly or through their health records (secondary use). Researchers continuously solicit participation from individuals that are representative of the population being studied. When individuals choose not to participate (or withhold or provide inaccurate PHI), this negatively impacts the analysis, interpretation and generalizability of the work. SC theory and trust-risk-intention beliefs have been empirically shown to influence a person's decision to provide personal information in an e-commerce environment [25;56]. As such, the Framework provides an ideal model for studying and understanding the public's attitudes regarding their PHI in primary care and health research contexts [25;56].

## Conclusion

The Trust-Risk Privacy Framework is a guide for understanding and anticipating the public's concerns about providing their PHI in both healthcare and health research contexts and specifically their privacy concerns in the areas of collection, control, transparency/awareness and appropriate authorization for the use of their PHI. Perceptions of how these variables are managed can either positively or negatively impact an individual's trust that PHI will be protected, or raise risk concerns that appropriate measures are not in place. The importance

of effective privacy protection in the EHRs context in general and health research specifically will be emphasized. The desired outcome will be to gain an understanding of the public's willingness to participate and provide accurate information in health research.

The next chapter examines the public's perceptions about the practices of data collection, control, transparency/awareness, preventing unauthorized access and authorization for health research (secondary uses) in EHRs. It shows how these views impact trust and risk beliefs and ultimately affect the public's intention to provide their PHI for both primary care as well as health research activities.

## REFERENCES

(1) Tri-Council Policy Statement: Ethical Conduct of Research Involving Humans - Second Edition, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (2012).

(2) Lowrance WW. *Privacy, confidentiality and health research.* Cambridge: Cambridge University Press; 2012.

(3) Willison D, Gibson E, McGrail K. **A Roadmap to Research Uses of Electronic Health Information.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011.

(4) Canadian Institutes of Health Research. CIHR Best Practices for Protecting Privacy in Health Research. Ottawa: Public Works and Government Services Canada; 2005. Date accessed 20/05/2006. www.cihr-irsc.gc.ca/e/29072.html

(5) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe.* Aldershot: Ashgate Publishing Limited; 2004.

(6) Institutes of Medicine. Protecting Data Privacy in Health Services Research. Washington D.C.: National Academy Press; 2009.

(7) Plomer A. *The Law and Ethics of Medical Research: International Bioethics and Human Rights.* New York: Routledge-Cavendish; 2005.

(8) Widdows H, Mullen C (editors). *The Governance of Genetic Information: Who Decides?* Cambridge: Cambridge University Press; 2009.

(9) Burgess MM, O'Doherty K, Secko D. Biobanking in British Columbia: discussions of the future of personalized medicine through deliberative public engagement. Personalized Medicine 2008;5(3):285-96.

(10) Willison DJ, Schwartz L, Abelson J, Charles C, Swinton M, Northrup D, . Thibane L. **Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public?** *J Am Med Inform Assoc* 2007;**14**:706-12. doi 10.1197/jamia.M2457

(11) Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM, Computerization of **Patient consent preferences for research uses of information in electronic medical records: interview and survey data.** *BMJ* 2003 Feb 15;326(7385):373. Date accessed: 17/05/2006 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC148897/pdf/373.pdf

(12) Canadian Institutes of Health Research (CIHR). Selected International Legal Norms on the Protection of Personal Information in Health Research. 2001.

(13) Knoppers BM. **Challenges in ethics review in health research.** *Health Law Review* 2009;**17** (2-3):47-52. Date accessed 07/03/2013. http://www.hli.ualberta.ca/en/HealthLawJournals/~/media/hli/Publications/HLR/17-23-06_Knoppers.pdf

(14) Gibson E, Brazi K, Coughlin MD, Emerson C, Fournier F, Schwartz L, et al. **Who's minding the shop? The role of Canadian research ethics boards in the creation and uses of registries and biobanks.** *BioMed Central Medical Ethics* 2008;**9**(17):1-9. Date accessed 11/04/2011, http://www.biomedcentral.com/1472-6939/9/17.

(15) Willison DJ. **Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward**. *Journal of Health Services Research and Policy* 2003;**8**(1):S1:17-S1:23 doi: 10.1258/135581903766468837

(16) Willison DJ. **Trends in collection, use and disclosure of personal information in contemporary health research: Challenges for research governance.** *Health Law Review* 2005;**13**(2&3):107-13.

(17) Assessing the Potential of National Strategies for Electronic Health Records for Population Health Monitoring and Research. Hyattsville, Maryland: U.S. Department of Health and Human Services, Centres for Disease Control and Prevention National Center for Health Statistics; 2006. Report No.: Series 2, Number 143.

(18) Black C, McGrail K, Fooks C, Baranek P, Maslove L. Data Data Everywhere...: Improving Access to Population Health and Health Services Research Data in Canada. Centre for Health Services and Policy Research 2005. Date accessed 07/08/2006, http://chspr.ubc.ca

(19) Al-Shahi R, Vousden C, Warlow C, and for the Scottish Intracranial Vascular Malformation Study (SIVMS) Steering Committee. **Bias from requiring explicit consent from all participants in observational research: prospective, population based study.** *British Medical Journal* 2005;1-5. Date accessed 21/10/05, http://www.bmj.com

(20) Tu V.J, Willison DJ, Silver FL, Fang J, Richards JA, Laupacis A, et al. **Impracticability of informed consent in the registry of the Canadian Stroke Network.** *New England Journal of Medicine* 2004; **350** (14):1414-21. www.NEJM.org

(21) Woolf S, Rothemich S, Marsland D. **Selection bias from requiring patients to give consent to examine data for health services research.** *Archives of Family Medicine* 2000;**9**:1111-8. www.archfammed.com

(22) Johnson N, Mant D, Jones L, Randall T. **Use of computerised general practice data for population surveillance: Comparative study of influenza data**. *British Medical Journal* 1991;**302**:763-5.

(23) El Emam, K., Fineberg, A. **An Overview of Techniques for De-Identifying Personal Health Information** (August 14, 2009). Available at *SSRN:* http://ssrn.com/abstract=1456490 or http://dx.doi.org/10.2139/ssrn.1456490

(24) Willison DJ, Emerson C, Szala-Meneok K, Gibson E, Weisbaum K, Fournier F, et al. **Access to medical records for research purposes: Varying perceptions across Research Ethics Boards.** *Journal of Medical Ethics* 2008. Apr; **34**(4):308-14. doi: 10.1136/jme.2006.020032

(25) Saxena N, MacKinnon M.P, Watling J, Willison D, Swinton M. Understand Canadian's Attitudes and Expectations: Canadians' Dialogue on Privacy and the Use of Personal Information for Health Research in Canada. Canadian Policy Research Networks: Public Involvement Network; 2006. Report No.: Pl09.

(26) EKOS Research Associates. Pan-Canadian Health Information Privacy and Confidentiality Framework Study. 2004.

(27) Council for International Organizations of Medical Sciences (CIOMS), World Health Organization (WHO). International Ethical Guidelines for Epidemiological Studies. Geneva; 2008. Date accessed 22/08/09, www.ufrgs.br/bioetical/cioms2008.pdf

(28) National Health and Medical Research Council, Australian Research Council, Australian Vice-Chancellor's Committee. National Statement on Ethical Conduct in Human Research. Government of Australia; 2007. Date accessed 04/11/09, www.nhmrc.gov.au/_files_nhmrc/file/publications/synopses/e72-jul09.pdf

(29) National Health and Medical Research Council, Australian Research Council, Universities Australia. Australian Code for the Responsible Conduct of Research. Australian Government; 2007.

(30) National Institutes of Health. Institutional Review Boards and the HIPAA Privacy Rule. United States: U.S Department of Health and Human Services; 2003. Date accessed 17/09/2006, http://privacyruleandresearch.nih.gov/pdf/HealthServicesResearchHIPAAPrivacyRule.pdf

(31) National Institutes of Health. Clinical Research and the HIPAA Privacy Rule. United States: U.S Department of Health and Human Services; 2004. Date accessed 17/09/2005, http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf

(32) The Academy of Medical Sciences. Personal Data for Public Good: Using Health Information in Medical Research. A Report from the Academy of Medical Sciences. London, England; 2006.

(34) The Bioethics Advisory Committee. Research Involving Human Subjects: Guidelines for IRBs. Singapore; 2004. Date accessed 12/06/10, www.bioethics-singapore.org/uploadfile/30038%20PMIRB%20Foreword.pdf

(35) United Nations Educational SaCOU. Universal Declaration on Bioethics and Human Rights. Paris, France: UNESCO; 2006. http://unesdoc.unesco.org/images/0014/001461/146180e.pdf

(36) World Health Organization (WHO). Operational Guidelines for Ethics Committees that Review Biomedical Research. Geneva; 2000. http://apps.who/tdr/publications/training-guideline-publications/operational-guidelines-ethics-biomedical-research/pdf/ethics.pdf

(37) World Health Organization (WHO). Handbook for Good Clinical Research Practice (GCP): Guidance for Implementation. Geneva; 2002. Date accessed 20/05/26. http://whqlibdoc.who.int/publications/2005/924159392X_eng.pdf

(38) Kosseim P. The Advent of Electronic Health Records (EHRs) in the Current Legal and Policy Context. Ottawa: Office of the Privacy Commissioner of Canada; 2005. Date accessed 09/06/2006. http://www.whqlibdoc.who.int/publications/2005/924159392X_eng.pdf

(39) Health Council of Canada (January 2005). Health Care: Renewal in Canada: Accelerating Change. 2005.

(40) Irving R. 2002 Report on Information Technology in Canadian Hospitals: Canadian Healthcare Technology. 2003.

(41) The Standing Committee on Social Affairs SaT, Kirby MJL. The Health of Canadians - The Federal Role Final Report. 2002.

(42) Electronic Health Records and the Personal Information Protection and Electronic Documents Act: University of Alberta, Health Law Institutes and University of Victoria, School of Health Information Science. Office of the Privacy Commissioner of Canada; 2005.

(43) Gibson E. Jewel in the Crown? *The Romanow Commission Proposal to Develop a National Electronic Health Record System.* Health Law Journal 2003;97-129.

(44) EKOS Research Associates. Healthcare and the Internet: Part of the Rethinking the Information Highway Study. Health Canada; 2003.

(45) Office of Health and the Information Highway. Toward Electronic Health Records. Health Canada 2001 January [cited 2005 Aug 15]; Available from: URL: http//www.hc-sc.gc.ca/ohih-bsi/

(46) Saxena SC, Kumar V, Giri VK. **Telecardiology for effective healthcare services**. *J Med Eng Technol* 2003 Jul;**27**(4):149-59.

(47) Flood CM, Thomas B. **Searching for a sweet spot: How do we trade off research benefits with health information privacy concerns?** In: Flood CM (Editor),

editor. Data Data Everywhere. Montreal, Que & Kingston, ON: McGill-Queen's University Press; 2011. p. 1-21.

(48) Levesque E, Leclerc D, Puymirat J, Knoppers BM. **Developing registries of volunteers: key principles to manage issues regarding personal information protection.** J Med Ethics 2010;**36**:712-4. doi:10.1136/jme.2010.036715

(49) Kosseim P. **Health research and data protection**. In: Flood CM (Editor), editor. Data Data Everywhere. Montreal, Que & Kingston, ON: McGill-Queen's University Press; 2011. p. 25-38.

(50) Government of Canada. Canadian Charter of Rights and Freedoms, Constitution Act, 1982, Part 1 of Schedule B to the Canada Act (1982).

(51) Privacy Act, R.S. 1985, c.P-21, Privacy Act, R.S. 1985, c.P-21, (2006).

(52) Personal Information Protection and Electronic Documents Act, S.C.2000, c.5, (2006). Date accessed 12/06/2008. http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

(53) Office of the Privacy Commissioner of Canada, Leading by example: Key developments in the first seven years of the Personal Information Protection and Electronic Documents Act (2008): Date accessed 12/06/08 www.priv.gc.ca/information/pub/lbe_080523_e.cfm.

(54) Gershon AS, Tu JV. **The Effect of Privacy Legislation on Observation Research: A Commentary**. In: Flood CM, editor. *Data Data Everywhere: Access and Accountability*? Montreal & Kingston: McGill-Queen's University Press; 2011. p. 73-9.

(55) Weisbaum KM, Slaughter PM, Collins PK. **A voluntary privacy standard for health services and policy research: Legal, ethical and social policy issues in the Canadian context**. *Health Law Review* 2005;**1**:42-6. Date accessed 11/05/2011. www.law.ulberta.ca/centres/hlidev1/userfiles/7_Weisbaum-Slaughter-Collins.pdf

(56) Malhorta NK, Kim SS, Agarwal J. Internet Users' Information Privacy Concerns (IUIPC): **The construct, the scale, and a causal model.** *Information Systems Research* 2004;**15**(4):336-55.

(57) Chafe R, Spencer P, Hudson M, Milnes K, Sullivan T. **Exploiting the secondary use of health data for effective cancer control: Opportunities and risks.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011. p. 151-170.

(58) Ells C, MacDonald C. **Implications of organizational ethics to healthcare**. *Healthcare Management Forum* 2002;**32**-9.

(59) Gostin LO. **Health Information Privacy.** *Cornell Law Review* 1995;**80**:451-528.

(60) Gostin LO, Turek-Brezina J, Powers M, Kozloff R. **Privacy and security of health information in the emerging health care system**. *Health Matrix: Journal of Law - Medicine* 1995;**5**(1):1-36.

(61) Griener G. **Electronic health records as a threat to privacy.** *Health Law Rev* 2005;**14**(1):14-7. PM:16538771

(62) Kosseim P, General Counsel Office of the Privacy Commissioner of Canada. The Advent of Electronic Health Records (EHRs) in the Current Legal and Policy Context. Ottawa, Ontario; 2005. Date accessed 09/06/2006. www.privcom.gc.ca/speech/2005/sp-d_051130_pk_e.asp

(63) Smith HJ, Milberg SJ, Burke SJ. **Information privacy: Measuring individuals' concerns about organizational practices.** *MIS Quarterly* 1996;**20**(2):167-96. www.jstor.org

(64) Stewart KA, Segars AH. **An empirical examination of the concern for information privacy instrument.** *Information Systems Research* 2002;**13**(1):36-49.

(65) Mason RO. **Four ethical issue of the information age.** *MIS Quarterly* 1986;**10**(1):4-12.

(66) Ajzen I. **The theory of planned behaviour.** *Organ Behavior Human Decision Processes* 1991;**50**:179-211.

(67) Ouellet R. **Privacy issues and the Canadian Medical Association** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011. p. 93-110.

(68) Martens P. **How and why does it "work" at the Manitoba Centre for Health Policy? A model of data linkage, interdisciplinary research and scientist/user interactions.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011. p. 137-150.

(69) Mayer RC, Davis JH, Schoorman FD. **An integrative model of organizational trust**. *Acad Management Rev* 2007;**20**(3):709-34.

(70) McKnight D, Cummings LL, Chervany NL. **Initial trust formation in new organizational relationships.** *Acad Management Rev* 1998;**23**(3):473-90.

(71) Fishbein M, Ajzen I. *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley; 1975.

(72) Culnan MJ, Bies RJ. **Consumer privacy online: Balancing economic and justice considerations.** *Journal of Social Issues* 2003;**59**(2):323-42.

(73) Milne GR, Gordon ME. **Direct mail privacy-efficiency trade-offs within implied social contract framework.** *Journal of Public Policy Marketing* 1993;**12**(2):206-15.

(74) Cohen RL. **Distributive justice: Theory and research**. *Soc Justice Res* 1987; **1**:19-40.

(75) Donaldson T, Dunfee TW. **Towards a unified conception of business ethics: Integrative social contracts**. *Acad Management Rev* 1994;**19**(2):252-84.

(76) Dunfee TW, Smith NC, Ross Jr. WT. **Social contracts and marketing ethics**. *J Marketing* 1999;**63(**July):14-32.

(77) Laufer RS, Wolfe M. **Privacy as a concept and a social issue: A multidimensional developmental theory.** *J Soc Issues* 1977;**33**(3):22-42.

(78) Health Information and Management Systems Society. Healthcare CIO Results: Health Information and Management Systems Society Foundation. 2004.

(79) Goldman J. Testimony before the subcommittee on health of the committee on ways and means on "Patient Confidentiality". 1998.

(80) Phelps J, Nowak G, Ferrell E. **Privacy concerns and consumer willingness to provide personal information.** *J Public Policy Marketing* 2000;**19**(1):27-41.

(81) Sheehan KB, Hoy MG. **Dimensions of privacy concern among online consumers.** J Public Policy Marketing 2000;19(1):62-73.

(82) Wulf KD, Odekerken-Schroder G, Iacocucci D. **Investments in consumer relationships: A cross-country and cross-industry exploration.** *J Marketing* 2001;**65**(October):33-50.

(83) Luo X. **Trust production and privacy concerns on the internet: A framework based on relationship marketing and social exchange theory.** *Indust Marketing Management* 2002;**31**(2):111-8.

(84) Sirdeshmukh D, Singh J, Sabol B. **Consumer trust, value, and loyalty in relational exchange.** *J Marketing* 2002;**66(**January):15-37.

(85) Cespedes FV, Smith HJ. **Database marketing: New rules for policy and practice.** *Sloan Management Rev* 1993;**34**(4):7-22.

(86) Milne GR, Rohm AJ. **Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives.** *J Public Policy Marketing* 2000;**19**(2):238-49.

(87) Gefen D, Karahanna E, Straub W. **Trust and TAM in online shopping: An integrated model.** *MIS Quarterly* 2003;**27**(1):51-90.

(88) Dowling GR, Staelin R. **A model of perceived risk and intended risk-handling activity.** *J Consumer Res* 1994;**21**(June):119-34.

**Title**

Over a decade of public trust: Canadians' opinion on privacy and electronic health information

**Authors**

Mary Lysyk
University of Ottawa
Institute of Population Health
1 Stewart St. Room 300
Ottawa, Ontario, Canada
K1N 6N5

Ian D Graham, PhD, FCAHS, Associate Professor
School of Nursing, University of Ottawa,
Senior Scientist, Ottawa Hospital Research Institute

Khaled El Emam, PhD, Associate Professor
Faculty of Medicine and the School of Information Technology and Engineering,
University of Ottawa

**Authors' Contributions**

I, the doctoral candidate (ML), assumed responsibility for this research project. I was responsible for the conceptualization of the project and led and conducted the different phases of the work including data collection, data analysis, overall synthesis and preparation of the manuscript.

Dr. Ian Graham (Associate Professor, School of Nursing) provided comments on the concept of the project, carefully reviewed the different drafts of this manuscript and approved the final manuscript.

Dr. Khaled El Emam (Associate Professor, Faculty of Medicine) also provided input on the concepts of the study and reviewed and provided feedback on manuscript drafts.

**Acknowledgements**

Elyse Gagné, University of Ottawa, provided copy editing for the completed manuscript.

**Funding**

In-kind funding support was provided by the Access to Information and Privacy Policy Department, Health Canada.

# CHAPTER 3:

# OVER A DECADE OF PUBLIC TRUST: CANADIANS' OPINION ON PRIVACY AND ELECTRONIC HEALTH INFORMATION


## Abstract

**Background**: Trust and confidence in the physician-patient relationship has been described as the cornerstone of medicine. As Canada moves to increase the use of electronic health records (EHRs) in the provision of health-care, protecting privacy and preserving confidentiality in the provider-patient relationship is becoming a greater priority. Given the potential of EHRs for health researchers, perceptions of trust in this context is also of high importance. Data detailing the effect of EHR systems on the physician-patient relationship and on other health care team members within and outside the circle of care are limited. Little is also known about public perceptions regarding the secondary uses of PHI from EHRs for health research purposes. An understanding of Canadians' opinions and experiences regarding personal health information is important for physicians, health researchers and other health-care team members and stakeholders, in order to fully appreciate and meet the public's expectations related to electronic health information privacy.

**Objectives**: The systematic review is designed to address several research questions: 1) What is the public opinion and experience regarding personal health information privacy and EHRs (according to the six dimensions of the Trust -Risk Privacy Framework)? 2) How much does the public trust physicians and health researchers to keep their personal health information safe and secure in EHR environments? How does this compare with others inside and outside the circle of care? And 3) What is the public opinion regarding privacy and access to personal health information for health research through the EHRs?

**Methods**: Medline, Embase and Cochrane Central Register of Controlled Trials, as well as the grey literature were searched for published public opinion surveys and questionnaires of public comfort levels with Electronic Health Information. Trends in six relevant outcome dimensions were analyzed. The six dimensions include public concerns over PHI: 1) control; 2) collection; 3) transparency & awareness; 4) preventing unauthorized access; 5) authorization for health research; and 6) trust and risk.

**Findings:** A review of over a decade (from January 1, 2000 to December 31, 2012) of public polling reveals 16 unique surveys totaling the responses of over 20,000 Canadians. This review shows that the public's view about electronic health information privacy remains strong and optimistic. At the heart of this largely positive view is the trust Canadian have in their physicians. This trust, in conjunction with low levels of reported incidents involving PHI, drives high comfort levels with electronic information sharing between health-care providers within the circle of care. However, this comfort and confidence does not automatically extend to health researchers or the secondary use of PHI for health research, even if data has been stripped of direct identifiers.

**Discussion**: The findings from this review are highly applicable to health-care providers and health-care organizations, health information custodians, and government agencies. As EHRs are increasingly being deployed across Canada and secondary uses for health research purposes are widely anticipated, findings are particularly important for members of the health research community. They provide evidence to support strong policy and practice related to PHI protection and caution when considering different consent models related to the secondary uses of health research.

## Background

Physicians have historically provided the first line of protection for their patients' health information [1-3]. As such, the commitment to protecting privacy and preserving confidentiality has been well established over several centuries and is considered sacrosanct within the doctor-patient relationship [1;4;5].

As Canada moves towards the implementation of electronic health record systems (EHRs) for providing care and for secondary uses such as health research, preserving confidentiality and privacy in the health-care provider-patient relationship becomes a priority more than ever [1]. Privacy commissioners, as well as the two major reviews of Canada's health-care system, have raised privacy as a key policy area that needs to be addressed [6-9]. It is critical to determine that information technology systems used at the point of care do not decrease patient trust or confidence [2]. Data detailing the effect of EHR systems on the physician-patient relationship and on other health care team members within and outside the circle of care are limited [2]. Little is also known about public perceptions regarding the secondary uses of PHI from EHRs for health research purposes [2].

An understanding of the public's opinion, attitudes, experiences and expectations regarding their personal health information (PHI) in EHR environments (for both primary care and secondary use) is therefore essential [2].

While numerous public opinion surveys have been conducted regarding information privacy in EHR environments, a review and synthesis of their findings has not been done. This makes it difficult for physicians and other health-care team members, health-care custodians and the health research community to fully understand and meet the public's expectations in this area. In this manuscript, we present a systematic review of national public opinion surveys.

The purpose of this review is to provide a summary of Canadians' views, attitudes, expectations and experiences in terms of privacy, confidentiality and security trust and risk

beliefs in EHR environments. Specifically, focus will be on both primary care and health research contexts, and any changes in perceptions that may have occurred over time.

**Research objectives**

The systematic review is designed to address several research questions:

1. What is the public opinion and experience regarding personal health information privacy, confidentially and security (according to a trust and risk beliefs framework) and EHRs?
2. How much does the public trust its physicians and health researchers to keep their personal health information safe and secure in EHR environments? How does this compare with other team members inside and outside the circle of care?
3. What is the public opinion regarding the secondary uses of personal health information for health research (as collected from EHRs)?

**Methods**

We searched Medline, Embase and Cochrane Central Register of Controlled Trials for published surveys and questionnaires of public comfort levels with Electronic Health Information. The review focuses on opinion surveys from January 1, 2000 to Dec 31, 2012. We also searched grey literature using the Internet search engine Google and examined stakeholder websites and contacted stakeholder groups. Trends were analyzed in six outcome dimensions relevant to understanding the public's priorities regarding privacy, confidentiality and security of personal health information (PHI) in electronic environments. The six dimensions comprise the Trust-Risk Theoretical Privacy Framework and include *collection* (equitable information exchange) of personal information is perceived to be fair only when the individual providing personal information is granted *control* (consenting to opt-in or the choice to opt-out). Furthermore, the individual should be informed about the organization's intended use of the personal information and thus there is a *transparency and awareness factor* (openness and awareness about established conditions and practices) with strategies to prevent unauthorized access as well as authorization for secondary uses such as health research [10, 11]. All of which are believed to increase trust and decrease risk beliefs related to the protection of PHI [10, 11]. The six dimensions will be presented as: 1)

control; 2) collection; 3) transparency and awareness; 4) preventing prevent unauthorized access; 5) authorization for health research (secondary uses); and 6) trust and risk [10;11].

***Inclusion/exclusion criteria***

Public opinion research surveys are included in the present review if they meet the following initial criteria: an original Canadian survey or Canadian public opinion research study; conducted between January 1, 2000 to December 31, 2012; national in scope; focus on privacy and electronic health information (search terms such as electronic medical files, electronic health records, Internet, e-health were included); or a privacy and secondary uses/health research focus; and published in English or French (**Table 3-1**). Conferences were searched and a cross-check was conducted to see if there was an ensuing journal publication or reports. Public opinion research and surveys that were provincial or regional or focused solely on information technology (such as email or Internet use) without reference to privacy and PHI were also excluded.

## Table 3-1: Medline Search Strategy

**Ovid Medline ® January 1, 2000 to December 31, 2012>**

**Search History**

| | |
|---|---|
| 1 | exp privacy |
| 2 | confidentiality |
| 3 | ethics |
| 4 | privacy.tw. |
| 5 | confidentiality.tw. |
| 6 | consent$.tw. |
| 7 | trust$.tw. |
| 8 | breach.tw. |
| 9 | unintended.tw. |
| 10 | (un-authori$ or unauthori$).tw. |
| 11 | secur$.tw. |
| 12 | or/1-11 |
| 13 | (electronic$ or digital$ or online or on-line or computer$).tw. |
| 14 | ((medical or health or research) adj2 (inform$ or record$ or data or chart$)).mp. |
| 15 | exp medical records/ |
| 16 | registries/ |
| 17 | health research/ |
| 18 | medical research/ |
| 19 | 13 and (14 or 15) |
| 20 | Medical Records Systems, Computerized/ |
| 21 | (Internet or e-health or tele-health or ehealth or telehealth or electronic health information or electronic medical files).tw. |
| 22 | or/17-19 |
| 23 | 12 and 20 |
| 24 | data sharing.mp. |
| 25 | or/23-24 |
| 26 | Questionnaires/ |
| 27 | exp Interviews/ |
| 28 | (perception or perceiv$ or opinion$ or attitut$ or confidenc$ or belief$ or trust$ or questionnair$ or focus group$ or interview$).tw. |
| 29 | or/26-28 |
| 30 | 25 and 29 |

**Additional database search histories are available upon request from the authors.**

### *Survey quality appraisal*

The reporting minimal disclosure criteria from the American Association of Public Opinion Research (AAPOR) that are generic in nature and relevant to Canadian public opinion research studies were used for the critical appraisal of the surveys [12]. These generic criteria are comprised of 19 items. Surveys were considered "high" quality if they reported at least 75% of the items, of "medium" quality if between 51%-75% were reported and "low" quality if less than 50% were reported. Survey quality appraisal was conducted by the author and applied to the full-text surveys.

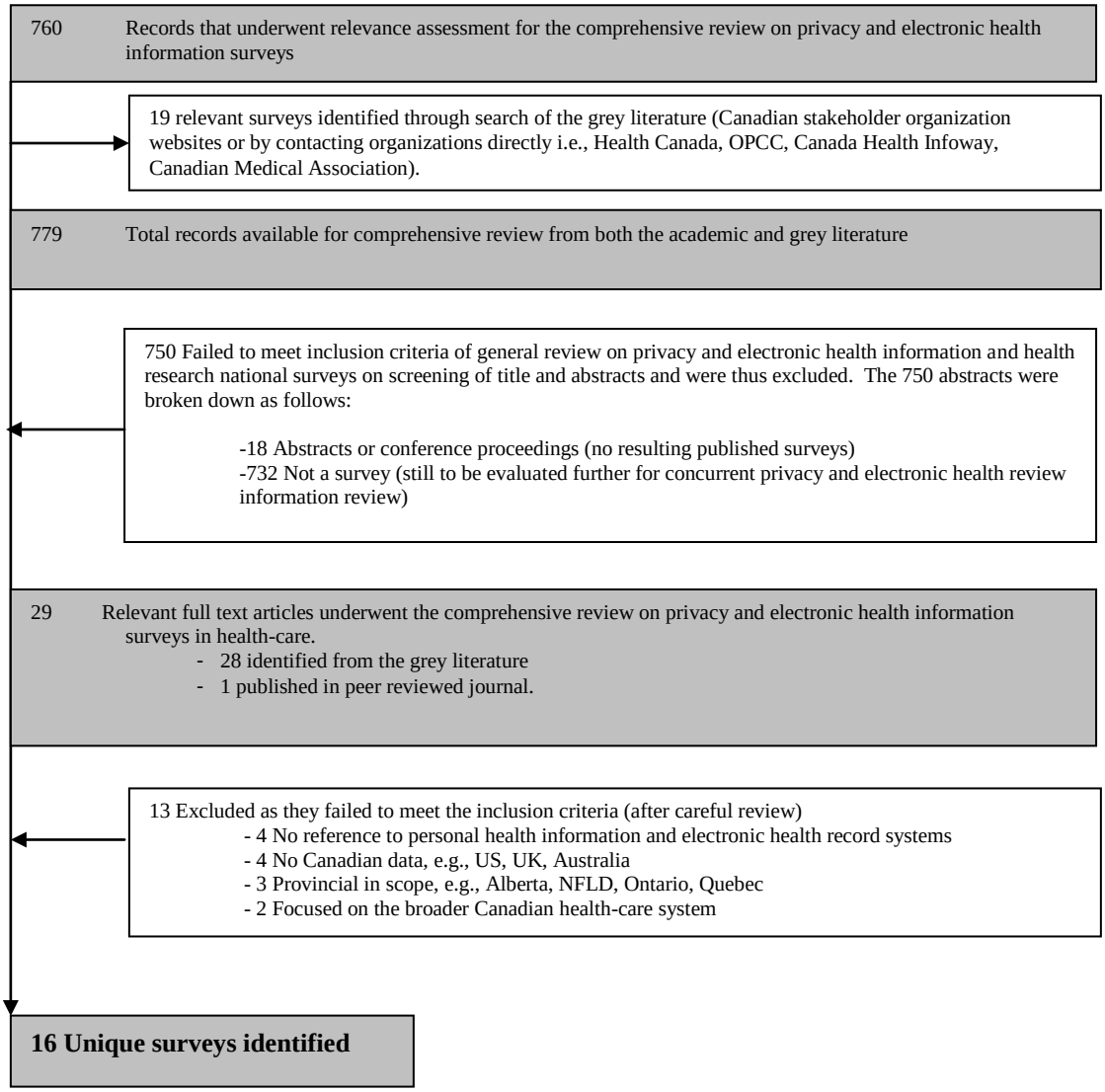
## Analysis

Questions from the surveys have been grouped according to the six privacy dimensions of the Trust-Risk Theoretical Privacy Framework. Descriptive analysis includes a detailed breakdown of questions and responses and an examination of trends where the same question was asked over time. The frequency distribution of responses with means, standard deviations, as well as overall study confidence intervals were reviewed.

## Findings

**Figure 3-1** provides a modified QUOROM flow diagram outlining the process for selection of surveys. It is from this pool of literature (a total of 779 articles) that the final 16 unique public opinion or other surveys were identified: one was a published article in scientific journal, and 15 were nonacademic surveys from the grey literature conducted by public opinion research firms. All were published between January 1, 2000-Dec 31, 2012. Though the search was extended until 2012, no national surveys published between 2010 and 2012 were found.

**Figure 3-1**
**Modified QUOROM flow chart for Canadian privacy and electronic health information surveys**




Survey characteristics are presented in **Table 3-2**. The sample sizes range from 1004-5182 participants. Quality scores are high and range from 15-17 (out of 19) of the AAPOR criteria. Confidence intervals are between +/- 1.4-3.1 percentage points 19 times out of 20. Telephone or mail-back surveys are the typical methodology being used.

Below is a summary of the key findings for each of the six privacy outcome dimensions. In terms of the notation used when citing results, the percent of public response will be presented first, followed by the year the survey was published, e.g., 59%, 2005.

**1) Control over PHI privacy in EHR systems**

Survey results reveal that protecting PHI privacy has been and continues to be important for Canadians (92%, 2002 & 2004) [22;23]. In fact, most agree that there are few types of information more important for privacy laws to protect, and this percentage has increased since 2005 (59% & 64%, 2005 & 2007) [16;18]. The majority of Canadians are concerned about the privacy of their PHI when shared among doctors using computer systems (67%, 2004) [23]. This concern has risen since 2002 when 63% of respondents identified this as an issue [22].

The majority of the public agree that knowledgeable "implied" consent is sufficient for physicians and other health-care providers to share PHI for direct patient intervention within the circle of care (80%, 2004) [15]. However, most of the public want greater health record access rights within an EHR system including: easy access to a health status summary (70%, 2004;84%, 2007), right to verify and report corrections to PHI (57%, 2003;65-70%,2004;68%, 2007), and the ability to hide or mask sensitive information (41%, 2003;55%, 2007) [15;18] All of these control elements have increased significantly (by at least 8 percentage points) since 2003 [13].

**Table 3-2: Summary of survey characteristics organized by polling firm and publication date alphabetically**

| *Syndicated or custom survey | Market research firm/ First author/Reference no. | Year published | Title | Methodology/Year survey conducted | Quality | Sample size |
|---|---|---|---|---|---|---|
| 1) Custom | Ekos Research Associates Inc. (for Canada Health Infoway) [13] | 2003 | Public Attitudes to Electronic Health Records and its Linkages | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2003 | High | 2006 |
| 2) Syndicated | Ekos Research Associates Inc. [14] | 2003 | Health Care and the Internet: Part of Rethinking the Information Highway Study | Wave 1:<br>Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2003 | High | 5182 |
| 3) Custom | Ekos Research Associates Inc. (for Health Canada) [15] | 2004 | Pan-Canadian Health Information Privacy and Confidentiality Framework | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2004 | High | 2500 |
| 4) Syndicated | Ekos Research Associates Inc. [16] | 2005 | Health Information and the Internet: Part of Rethinking the Information Highway Study | Wave 2:<br>Self-administered mail-back survey sent to consenting telephone survey respondents<br>Conducted: 2005 | High | 3467 |
| 5) Custom | Ekos Research Associates Inc. (for The Office of the Privacy Commissioner of Canada) [17] | 2006 | Revisiting the Privacy Landscape a Year Later | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2006 | High | 1020 |

| *Syndicated or custom survey | Market research firm/ First author/Reference no. | Year published | Title | Methodology/Year survey conducted | Quality | Sample size |
|---|---|---|---|---|---|---|
| 6) Custom | Ekos Research Associates Inc. (for Health Canada, Canada Health Infoway, The Office of the Privacy Commissioner of Canada) [18] | 2007 | Electronic Health Information and Privacy Survey: What Canadians Think - 2007 | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2007 | High | 2469 |
| 7) Custom | Ekos Research Associates Inc. (for the Office of the Privacy Commissioner of Canada) [19] | 2007 | Canadians and the Privacy Landscape a Year Later | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2007 | High | 2001 |
| 8) Syndicated | Ekos Research Associates Inc. [20] | 2007 | Graphical Summary Report: Part of the Information Highway Study | Wave 1:<br>Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2007<br><br>Wave 2:<br>Self-administered mail-back survey sent to consenting telephone survey respondents<br>Conducted: 2007 | High | 4542<br><br>1581 |
| 9) Custom | Ekos Research Associates Inc. (for the Office of the Privacy Commissioner of Canada) [21] | 2009 | Canadians and Privacy | Telephone survey with a stratified national random sample, 16 years and over<br>Conducted: 2009 | High | 2028 |

| *Syndicated or custom survey | Market research firm/ First author/Reference no. | Year published | Title | Methodology/Year survey conducted | Quality | Sample size |
|---|---|---|---|---|---|---|
| 10) Syndicated | IBM Business Consulting Services [22] | 2002 | Health Insider. Survey No. 8 | Telephone survey with a stratified national random sample, 15 years and over<br>Conducted: 2002 | High | 2565 |
| 11) Syndicated | IBM Business Consulting Services [23] | 2004 | Health Insider. Survey No. 11 | Telephone survey with a stratified national random sample, 15 years and over<br>Conducted: 2004 | High | 2565 |
| 12) Custom | Ipsos Reid (for the Canadian Medical Association) [24] | 2007 | Canadians' Views of Privacy | Telephone survey with a stratified national random sample, adults<br>Conducted: 2007 | High | 1004 |
| 13) Syndicated | Pollara Research [25] | 2005 | Health Care in Canada Survey 2005 | Telephone survey with a stratified national random sample, 18-91 years<br>Conducted: 2005 | High | 1207 |
| 14) Syndicated | Pollara Research [26] | 2006 | Health Care in Canada Survey 2006 | Telephone survey with a stratified national random sample, 18-91 years<br>Conducted: 2006 | High | 1004 |
| 15) Syndicated | PriceWaterHouseCooper [27] | 2000 | Health Insider. Survey No. 4 | Telephone survey with a stratified national random sample, 15 years and over<br>Conducted: 2000 | High | 2592 |

| *Syndicated or custom survey | Market research firm/ First author/Reference no. | Year published | Title | Methodology/Year survey conducted | Quality | Sample size |
|---|---|---|---|---|---|---|
| 16) Academic research | Willison D. et al [28] | 2007 | Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public? | Computer aided telephone survey of a representative national sample, 18 years and over<br>Conducted: 2005 | High | 1230 |

*Custom public opinion research is research that a stakeholder organization commissions and owns. In contrast, research firms own the copyright for syndicated studies, which are typically sponsored by multiple stakeholder groups.

**2) Concern over health information custodians' collection of PHI in EHR systems:**
Few Canadians are concerned about giving their PHI to health-care custodians such as doctors or hospitals (19%, 2007) [19]. Most are comfortable with an EHR system being used to collect and store PHI (70%, 2005; 71%, 2003), however, this comfort has decreased since 2000 (83%, 2000) [14, 16, 27]. Concern increases when sensitive information such as sexually transmitted diseases (45%, 2003); illicit drug use (46%, 2003); or mental health history (49%, 2003) are being disclosed [13]. Basic health information such as weight and blood pressures were of the least concern (29%, (2003) [13]. Interestingly, 40% of respondents expressed concern over direct identifiers such as name, address and age being in an EHR (2003) [13].

In comparison with paper-based systems, 55% (2007) of the public feel that EHRs are better at ensuring the security of patient information collected and 48% (2007) feel EHRs would be better at protecting privacy (increased from 40%, reported in 2003) [18].

**3) Transparency and awareness of PHI privacy, confidentiality and security practices**
In terms of the transparency of health information custodian privacy practices, a majority think that notices, brochures and pamphlets in doctors' offices would be effective as a way of informing the public (72%, 2004) [15]. However in the same survey, almost 8 in 10 indicate that they have not read any of these publications when available (77%, 2004) [15]. Of those that have read them, a resounding majority, 84% (2004) find them to be effective [15].

Regarding awareness of privacy laws and oversight bodies, 60% (2007) report that they are not aware of any privacy laws that protect their PHI [18], while 66% (2009) state they are not aware of the presence of privacy oversight organizations [21]. Of note, awareness of the latter has improved by 12 percentage points since 2005 [16].

**4) Preventing unauthorized access to PHI in EHR systems**
Over the last 10 years, when asked if they have enough information to know how new technologies might affect personal privacy, only half of the public (50%) consistently agree they do; half do not (mean 50%, 2000-2009) [21]. However, the vast majority of the public

are at least somewhat concerned about the impact of new technologies on personal privacy (90%, 2009) [21]. Three areas of concern with electronic health information and the EHR are: unauthorized access for malicious reasons (45%, 2007); unauthorized uses of PHI (42%, 2007); and human error (37%, 2007) [18].

A large percentage of Canadians support enhanced measures to safeguard privacy and security of PHI in electronic environments and prevent unauthorized access (65%-77%;2007) [18]. These measures include: knowing that health-care providers must adhere to security safeguards (72%, 2004); support for access control measures and audit trails (72%,2003;77%; 2007); new legislation and strong penalties for unauthorized access (66%,2003 ;71%,2004;74%;2007); breach notification (70%, 2007); accessible privacy policies (59%,2003; 66%,2007); and implementation of breach management protocols (65%, 2007) [13,15,18]. Protective measures first identified in 2003 or 2004, show even greater support in 2007 [13;15;18].

**5) Authorization for Health Research (secondary use of PHI in EHR systems)**

The Canadian public would be alarmed if protecting privacy would make conducting health research (secondary uses of data) difficult or impossible (89%, 2007) [28]. The public values both health research and their information privacy. Support for the release of PHI with consent is high (74%, 2007) [24]. Support increases to 84% when direct identifiers have been removed (84%, 2007) [18]. However, the findings are less clear when it comes to releasing PHI data stripped of direct identifiers without consent. The one national study that explores this question in detail finds that the public will consider different consent options, but in the end acceptable consent must be obtained (9% prefer not using de-identified data without consent, 36% would like their permission to be sought, 28% would require notification, and 27% would be willing for their data to simply be used without their consent or notification; 2007) [28]. This is also the case for data linkage with de-identified data sets, e.g., linking health research with income data, 27% do not use, 40% ask permission first, 16% require notification, 17% just use it; 2007 [28].

**6) Trust and risk beliefs**

The Canadians' trust in physicians keeping their PHI safe and secure has remained strong since 2004 (88% 2004; 91%, 2004); 86% 2007) [15;18;23]. While trust that physicians will keep PHI safe and secure does not fall below 86% in public opinion surveys, trust that health researchers will do the same is significantly lower: health researchers in universities (57% 2004; 52% 2007); government health researchers (54% 2004; 52% 2007); private sector health researchers (46% 2004; 45% 2007) [15;18]. This is despite the fact that health researchers typically deal with much less identifiable information than physicians have access to [34-36]. Given the relative low trust levels for most types of health research, it is interesting that the public is largely comfortable with (or supports) the use of their electronic health information in the administration of the health-care system without their expressed consent, e.g., address public health issues (71%, 2007); plan, monitor and evaluate the health-care system (61%, 2005; 60% 2006;74%, 2007); prevent improper use of the health-care system (71%, 2007) [18;24;25]. Some results such as to plan, monitor and evaluate the health-care system that have been tracked since 2005, have observed a significant increase in support [18;24;25]. These results have also been confirmed by other studies that show that using PHI (without consent) to improve quality care (86%, 2007) and to track communicable diseases (89%, 2007) is acceptable [28]. Conversely, a majority of Canadians do not support the use of their PHI internally in hospital fundraising activities (62%, 2004) or spiritual counselors, e.g., hospital chaplain, (78%, 2004) without express consent of the individual [15]. This is despite the fact that hospital chaplains and other spiritual counselors are functioning from the same institution as physicians in these survey questions.

Few Canadians report having recently (within the past year) withheld information or opting not to see a health-care provider over concerns about their health information privacy (2-5%, 2007) [20]. A larger percentage of Canadians state that they have, at some time in their lives, withheld PHI over privacy concerns (12%, 2003; 11%, 2007;) [13,24]. This percentage represents approximately 3.5 million adult Canadians and has changed little since the question was first asked in 2003 [13].

In 2007, 4% of Canadians reported they had experienced a breach of their PHI, the majority indicated that their information was not held in confidence or was released without consent [18].

## Discussion

### *Chief findings*

This study builds on over a decade of public opinion research by summarizing the key findings from these studies according to the Trust-Risk Theoretical Privacy Framework. This provides a greater and more in-depth understanding of the determinant of trust, particularly how the six dimensions relate to the release of PHI for primary care and health research through the EHRs. Over the past decade in Canada, there has been strong public support for the concept of an EHR and high trust that PHI will be kept safe and secure [15;18;23;24]. As well, PHI privacy awareness has been increasing [21]. The latter is due in large part to significant efforts by the federal and provincial privacy commissioners and oversight organizations.

However, this positive picture should be viewed with caution. For example, Canadians have serious concerns regarding access rights and the lack of breach notification procedures [18]. As well, the public expressed some hesitations related to disclosing more sensitive PHI data in EHR environments [13]. Of greatest concern is unauthorized access, unauthorized use and the possibility of human error leading to accidental disclosures [18]. Canadians also worry that they do not entirely understand the potential risks that technology poses to personal information [21]. The public appears to need more information and greater transparency in terms of understanding actual EHR threats and risks to privacy, confidentiality and security.

As privacy breaches and related violations may result in harm to the patient (intrinsic, consequential and economic harm), the outcomes of this review are particularly relevant for physicians for whom trust and satisfaction in the physician-patient relationship has been described as the cornerstone of medicine [2;3;37]. As the sixth dimension in the Trust-Risk Theoretical Privacy Framework suggests, lack of trust resulting from unauthorized or accidental disclosures of PHI engenders what has been described in the literature as a

"chilling effect" [3;38]. This is related to the perceived risk that prevents patients from fully communicating about their health problems to their health-care provider or from seeking appropriate and timely intervention [3;38].

In the US, the behaviour of withholding PHI from health-care providers is notably higher. A 2007 survey found that as many as 17% of adults have changed their behaviour to protect their privacy, for example by withholding information from the health-care providers [39]. More than a quarter of teens indicate that they would not seek out health-care if they had concerns about their information confidentiality [40]. In a survey of physicians in the US, nearly 87% report that a patient has asked that information be kept out of their record, and nearly 78% of physicians said that they have withheld information from a patient's record due to privacy concerns [41].

Unlike the primary care context, high trust and confidence does not automatically extend to health researchers or the secondary uses of data for health research purposes. Canadians recognize and desire the benefits that research offers. But they also want to protect the privacy and maintain control of their PHI, even if direct identifiers have been removed [28]. The public is willing to share PHI information for health research and will consider different consent options, but they believe that acceptable consent must be obtained [28].

***Limitations of the research***

All of the survey results must be viewed within a health-care system with an emerging, incremental adoption of EHRs. Survey results are largely based on perceptions and attitudes as opposed to actual patient experiences with these systems [18;42-44]. Furthermore, as survey reliability and validity were typically not reported, they could not be ascertained in this study.

Next, the grouping of survey questions according to the six dimensions of the Trust-Risk Theoretical Privacy Framework could only be done subjectively as objective guidelines or protocols do not exist regarding the dimensions. However, replication of the selection and

grouping of the questions would greatly add to both the reproducibility and assurance that the questions reflect the dimensions they are intended to.

***Policy implications and directions for future research***

Key policy implications related to the dimensions of the Trust-Risk Privacy Theoretical Framework are offered in **Table 3-3**. They are derived directly from the findings of the systematic review and provide empirical support and validity to privacy protection measures that, at a minimum, need to be in place.

Future research must engage the public to further explore and better define what construes "acceptable" consent models. This will add greatly to the development of policy and practice in this complex and highly sensitive area. As well studies that focus on actual public experiences in EHR environments are now needed in order to confirm actual (versus perceived) threats to privacy, confidentiality and security.

**Table 3-3: Key recommendations and application to privacy policy and practice**

## Control

- Develop policies and procedures to receive and respond to patients' requests to access, verify and report corrections to electronic health records and respond to requests to restrict access to specific components of their records, e.g., hiding or masking sensitive information;

## Collection

- Ongoing emphasis related to collecting only the PHI that is needed for care and/or health research, particularly as it relates to more sensitive medical data;

## Transparency

- Inform patients of their privacy rights and the privacy practices and policies of the health-care custodian/organization through a comprehensive communication plan. This should include where to turn if patients have privacy concerns or if they feel that their privacy rights have been violated. Patient-education programs should also be considered;

## Preventing unauthorized access

- Provide ongoing training to all staff regarding organizational privacy, confidentiality and security practices in order to decrease the likelihood of human error;

- Implement regular and ongoing independent system evaluation and audit of privacy, confidentiality and security practices. This will help identify gaps and ease public concern that unauthorized access will occur or that privacy and security procedures will not be followed. Audit outcomes should be made available to the public to promote transparency and awareness;

- Provide explicit notification to both the individual and, if appropriate, the privacy oversight body, e.g., provincial privacy commissioner, in the event of a breach of PHI (regardless of whether information is deemed sensitive or not) and establish organizational breach protocols to effectively manage breaches once they have occurred;

## Authorization for health research (secondary uses from EHRs)

- Public support for the secondary uses of PHI (with consent) increases when data that has been de-identified as much as possible.
- Further public consultation is needed to explore different consent/notification models regarding access to de-identified data.

## Conclusion

Privacy and security of PHI in information technology environments is more complex today than ever before. Public opinion remains positive and trust is strong that PHI will be protected when EHR systems are used in primary health-care. This trust does not automatically transfer to health researchers or the secondary uses of PHI from these systems. As EHRs will likely become the primary source for data collection in the future, further study of attitudes, EHR threats and risks, along with consent models deemed "appropriate" by the public is needed.

Protecting trust in EHR systems is paramount. If trust is lost, it is the physician-patient relationship that will be affected first and likely suffer the most, followed by lost opportunities to improve health through research. This study offers basic pragmatic policy guidance to help avoid these scenarios.

## REFERENCES

(1) Davis L, Domm JA, Konikoff MR, Miller RA. **Attitudes of first-year medical students toward the confidentiality of computerized patient records.** *Journal of the American Medical Informatics Association* 1999;**6**(1):53-60.

(2) Garrison GM, Bernard ME, Rasmussen NH. **21st-century health care: the effect of computer use by physicians on patient satisfaction at a family medicine clinic.** Fam Med 2002 May;**34**(5):362-8.

(3) Harris RE. **The need to know versus the right to know: privacy of patient medical data in an information-based society**. Suffolk Univ Law Rev 1997;**30**(4):1183-218.

(4) Code of Ethics, Canadian Medical Association, (2004).

(5) Etziony MB. *The Oath of Hippocrates. The Physician's Creed: An Anthology of Medical Prayers, Oaths, and Codes of Ethics Written and Recited by Medical Practitioners through the Ages.* Springfield, Illinois: Charles C. Thomas; 1973.

(6) Privacy Commissioner of Canada. Condition Critical: Health Privacy in Canada Today. 2006. Date accessed 03/09/2006. www.privcom.gc.ca/speech/02_05a_0100618_e.asp

(7) Commission on the Future of Health Care in Canada, Romanow RJ. Building on Values: The Future of Health Care in Canada Final report. Saskatoon: Commission on the Future of Health Care in Canada; 2002. www.hc-sc.gc.ca/english/care/romanow/index.html

(8) The Standing Committee on Social Affairs SaT, Kirby MJL. The Health of Canadians-The Federal Role Final Report. 2002. Date accessed 03/08/2006. www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/SOCI-E/rep-e/repoct02vol6-e.htm

(9) Office of Health and the Information Highway. Toward Electronic Health Records. Health Canada 2001 January [cited 2005 Aug 15]. Date accessed 15/08/2005. www.hc-sc.gc.ca/ohih-bsi/

(10) Malhorta NK, Kim SS, Agarwal J. **Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model.** *Information Systems Research* 2004;**15**(4):336-55.

(11) Smith HJ, Milberg SJ, Burke SJ. **Information privacy: Measuring individuals' concerns about organizational practices.** *MIS Quarterly* 1996;**20**(2):167-96. www.jstor.org

(12) AAPOR [no date listed]. Home page of the American Association of Public Opinion Research (AAPOR). 2012. Date accessed 25/10/2012. www.aapor.org

(13) EKOS Research Associates Inc. Public Attitudes to the EHRs and Its Linkages. 2003.

(14) EKOS Research Associates. Healthcare and the Internet: Part of the Rethinking the Information Highway Study. Health Canada; 2003.

(15) EKOS Research Associates. Pan-Canadian Health Information Privacy and Confidentiality Framework Study. 2004.

(16) Harris Interactive. Health information privacy (HIPAA) notices have improved public's confidence that their medical information is being handled properly. 2005. www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=894

(17) EKOS Research Associates Inc. Revisiting the Privacy Landscape a Year Later. 2006.

(18) EKOS Research Associates Inc. Electronic Health Information and Privacy: What Canadians Think-2007. 2007.

(19) EKOS Research Associates Inc. Canadians and the Privacy Landscape a Year Later. 2007.

(20) EKOS Research Associates Inc. Wave 1 and Wave 2: Graphical Summary Report: Part of the Information Highway Study. 2007.

(21) EKOS Research Associates Inc. Canadians and Privacy. 2009.

(22) IBM. HealthInsider - Medical Records. 2002. Report No.: Survey No. 8, Section 9.

(23) IBM. HealthInsider. 2004. Report No.: Survey No.11.

(24) Ipsos Reid. The Canadian Medical Association: Canadian Views on Privacy. 2007.

(25) Pollara: Strategic public opinion and market research. Health Care in Canada Survey 2005: A national survey of health care providers, managers and the public. 2005. Date accessed 12/08/2007. www.hcic.sssc.ca

(26) Pollara: Strategic public opinion and market research. Health Care in Canada Survey 2006: A national survey of health care providers, managers and the public. 2006. Date accessed 12/08/2007. www.hcic.sssc.ca

(27) PriceWaterhouseCoopers. HealthInsider: An in-depth research report on consumer health issues. 2000. Report No.: No. 4.

(28) Willison DJ, Schwartz L, Abelson J, Charles C, Swinton M, Northrup D, Thibane L. **Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public?** *J Am Med Inform Assoc* 2007;**14**:706-12. Doi 10.1197/jamia.M2457

(29) EDS. EDS Canada Privacy and Identity Management Survey White Paper: Summary of Results and Findings. 2005.

(30) EKOS Research Associates Inc. Canadians and the Privacy Landscape. 2007.

(31) Grimes-Gruczka T, Gratzer C. *Ethics survey of consumer attitudes about health websites*. California Health Care Foundation; 2000.

(32) Siegler M. **Confidentiality in medicine - a decrepit concept**. *New England Journal of Medicine* 1982;**307**(24):1518-21.

(33) Mole D, Fox C. **Electronic data protection: Procedures need drastic improvement.** *British Medical Journal* 2005 May **3**;330:537.

(34) Willison DJ. **Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward**. *Journal of Health Services Research and Policy* 2003;**8**(1):S1:17-S1:23.

(35) Willison DJ. **Trends in collection, use and disclosure of personal information in contemporary health research: Challenges for research governance.** *Health Law Review* 2005;**13**(2&3):107-13.

(36) Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM, Computerization of **Medical Practices for the Enhancement of Therapeutic Effectiveness investigators. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data.** *BMJ* 2003 Feb **15**;326(7385):373.

(37) Day B. **Why are doctors so concerned about protecting the confidentiality of patient's records?** *Healthcare: Information Management & Communications Canada* 2008;**22**(N0.2):36-7.

(38) Gostin LO. **Health Information Privacy.** *Cornell Law Review* 1995;**80**:451-528.

(39) The Harris Poll. Many U.S. Adults are Satisfied with Use of Their Personal Health Information. 2007. Report No.: #27. Date accessed 07/08/2008. www.harrisinteractive.com/harris_poll/index.asp?PID=743

(40) Cheng T, Savageau J, Sattler J, DeWitt A, Thomas G. **Confidentiality in health care: A survey of knowledge, perceptions, and attitudes among high school students.** *Journal of the American Medical Association* 1993;**269**(11):1404-8.

(41) Association of American Physicians and Surgeons. New poll: Doctors lie to protect patient privacy. 2001. www.aapsonline.org/press/nrnewpoll.html. Archived at www.webicitation.org/5NzROMX2

(42) Canadian Institutes for Health Information (CIHI). Understanding Family Physician Usage of Electronic Health Records in Canada: Results From the 2004 National Physician Survey: Analysis in Brief. 2006. www.cihi.ca

(43) The College of Family Physicians of Canada CMATRCoPaSoC. National Physician Survey, 2007. Date accessed 05/02/2008. www.nationalphysiciansurvey.ca/nps/2007_Survey/Results/physician1-e.asp

(44) The Commonwealth Fund. **New International Survey of Primary Care Physicians. Health Affairs:** The Policy Journal of the Health Sphere 2006. http://content.healthaffairs.org/cgi/content/abstract/hlthaff.25.w555

## Title

A comparison of international and Canadian guidelines in protecting personal health information in health research

## Author

Mary Lysyk
University of Ottawa
Institute of Population Health
1 Stewart St. Room 300
Ottawa, Ontario, Canada
K1N 6N5

## Author's Contribution

I, the doctoral candidate (ML), assumed responsibility for this research project. I was responsible for the conceptualization of the project, and led and conducted the different phases of the work including data collection, data analysis, overall synthesis and preparation of the manuscript.

## Acknowledgements

I am grateful for the supervision I received by Dr. Ian Graham (Associate Professor, School of Nursing) who provided comments on the concept of the project and carefully reviewed the different drafts of this manuscript. Elyse Gagné, University of Ottawa, provided copy editing for the completed manuscript.

Patrick Moreau (PM), Research Assistant, Access to Information and Privacy Policy Department, Health Canada, provided independent eligibility for inclusion review of the international documents for both the original 2011 and revised manuscript. As well, he replicated the search strategy in the original manuscript and verified the items of the CIHR BPPP list at that time. John Horovath, (JH), CIHR Privacy Advisory Committee member & Senior Policy Advisor, Access to Information and Privacy Policy Department, Health Canada, also independently verified the items of the CIHR BPPP list.

## Funding

In-kind funding support was provided by the Access to Information and Privacy Policy Department, Health Canada.

# CHAPTER 4:

# A COMPARISON OF INTERNATIONAL AND CANADIAN GUIDELINES FOR PROTECTING PERSONAL HEALTH ONFORMATION IN HEALTH RESEARCH


## Abstract

**Background:** While health research activities exemplify some of the greatest hopes for improved health-care, they also highlight public concerns for the protection of personal-level health data that is collected, used and stored.

**Objectives**: To identify and compare policy and guidance documents and their specific guidelines for personal health information (PHI) protection in health research internationally with those in Canada. The specific objectives are to 1) compare international fair information principles (FIPs) with the Canadian Standards Association (CSA) Model Code 10 Privacy Principles; 2a) examine how international and Canadian guidance documents based on FIPs compare with those derives from ethics principles alone, 2b) compare international documents and their guidelines, i.e., specific practice items, with those in Canada; finally, 3) identify and analyze additional privacy protection items from the international documents.

**Methods:** This descriptive study reviews relevant international and Canadian documents on PHI protection for health research available in the public domain in order to identify those that are broadly known to either the privacy or health research communities. The documents were searched from an unspecified start date until January 01, 2013.

The two Canadian policy and guidance documents were converted in this article to a "practice item list" of privacy practice guidelines, i.e., "items". This would allow for international guideline-by-guideline comparative analysis with the Canadian context.

**Findings**: Twenty eight international documents were identified. Those that were derived from both FIPs and ethics principles (five of 28) show the largest number of common practices with comparable Canadian policy and guidance documents which are also based on

both of these concepts. Documents from the United Kingdom are the most comparable with the Canadian documents, followed by Singapore, the United States and CIOMS.
In terms of additional practices, five themes (elements) have emerged with 100 practice guidelines identified.

These additional elements and their practice guidelines are consistent with those seen in other sectors, e.g., e-commerce, private sector, and government, related to managing and coping with advancing technologies and subsequent threats to information privacy. As well, it should be noted that most are essentially further specifications to those found in the TCPS 2.

**Discussion**: The listing of the 100 additional practices guidelines can be emulated, modified or rejected in future revisions of the TCPS 2 or CIHR BPPP in order to address the challenges faced with advances in information technology, calls for harmonization and the public's desire for greater privacy protection.

## Introduction

Health research is the single vehicle to uncover and understand the varying causes of disease or illness, the broader determinates of health and to discover new or to validate traditional ways of treating or managing individuals who suffer from these conditions [1-3]. Health research activities are thus at the heart of medical, health and scientific developments [4]. While they hold some of the greatest hopes for improved health-care, health research activities also highlight public concerns for the protection of personal health information (PHI) that is collected, used and stored electronically [2;3;5-8].

## Background

Advances in information technology and the increasing pace of international collaborative studies have raised challenging issues to privacy protection in health research [9]. Over the past three decades, these issues have forced a global revision of international privacy laws, policies and practices [2;3;9-10]. These revisions have included the use of data protection principles with a view towards balancing the rights of the individual to privacy, with legitimate societal uses of personal health information (PHI) [2;3;9-11].

Like the international community, the Canadian public also desires a balanced approach to privacy protection in health research [12-14]. While the public supports health research activities, Canadians feel that PHI, along with personal financial information, is of the most sensitive information there is about an individual [12-21]. Concerns about maintaining the privacy and confidentiality of PHI are particularly important in both primary care and health research contexts, where individuals can disclose especially sensitive information, such as information about their mental health, their alcohol and substance abuse and their sexual practices that would result in harm should their privacy be breached or violated [22-24].

Health information privacy breaches are not typically related to physical, but rather psychosocial harms [24;25]. For example, psychosocial harms can include stigmatization, discrimination, disruptions to family, work or social life and loss of trust in the health-care system [24;25]. Loss of trust leads to an increased likelihood of not seeking necessary healthcare, or not disclosing sensitive but critical information to health-care providers; in

terms of health research, there is a potential loss of willingness to participate in future research studies [24;25]. As such, psychosocial harms are of significant concern, and maintaining public trust in health research is imperative [24;25].

***Ethics and fair information principles in health research***

Ethics principles developed from post-World War II human rights documents, with an aim to "promote and preserve the dignity and worth of the human person and respect for and observance of fundamental freedoms", form the foundation of health research standards today [3;9;26]. Privacy is a fundamental principle of ethics and human rights laws [3;9;26]. Despite national and international efforts towards a harmonization of ethics principles, there is a wide variation in the laws, standards and norms regulating health research both within and across Canada, the US, the UK, Australia, the European Union and Asia-Pacific countries, among others [3;9;26]. Currently, the vast majority of nations around the globe protect privacy in their constitutions [31]. In Germany, *Informationsselbstbestimmung* (informational self-determination or control right) was given constitutional status as early as 1949 [32]. In countries such as in Canada, the US, France, Japan and India where privacy is not mentioned directly in constitutions, the courts recognize implicit constitutional rights to privacy [32].

While "privacy" refers to the rights of the individual, the control of personal information today implies an obligation for organizations to safeguard all personal information entrusted to them [10;27;32]. As such, information privacy protection has evolved to include a number of "Fair Information Principles" (FIPs). FIPS are aimed at protecting privacy in the digital era and are different from post-World War II ethics principles and human rights laws [10;32].

There have been many concerns internationally from sectors such as finance, industry and government that the present FIPs have not kept pace with the rapid technological developments beyond the Mainframe Era [28-30].

While much is known about the impact of FIPs on the development of privacy statutes, in terms of health research, researchers know little about what degree FIPs are actually used to

form the basis for privacy protection practices outlined in health research policy and guidance documents. Nor is it known whether or not the use of FIPs leads to greater harmonization and a more comprehensive approach to addressing the privacy issues related to advancing technologies.

This study analyzes international privacy policy and guideline documents used in health research with an emphasis on electronic health information (specifically in terms of prospective broad-use data bases and the secondary uses of PHI). It compares these international documents to the relevant Canadian documents, and highlights the role of FIPs in the development of these practices. A mapping of similarities, differences and trends at the practice level is presented. As well, the study identifies any additional provisions from the international community demonstrating how health research privacy, confidentiality and security challenges and issues are being addressed in other jurisdictions.

**Research objectives**

The overall objective of this descriptive study is to identify and compare policy and guidance documents for PHI protection in health research internationally with those in Canada.

Specific objectives are as follows:

1) To provide a comparative analysis of international FIPs with the Canadian Standards Association (CSA) Model Code 10 Privacy Principles.

2) a) To examine how international and Canadian guidance documents based on FIPs compare with those derived from ethics principles alone. As well, to compare those documents that are specific to privacy protection with those where privacy protection is embedded within broader health research practices guidelines.

b) To compare the international and Canadian health research guidance documents and their specific practice items. Particular attention will be paid to provisions related to

primary and secondary uses of data and the establishment of prospective databases for broad use in research.

c) To create a listing of additional privacy protection guidelines derived from the international documents.

## Conceptual framework

The Trust-Risk Privacy Theoretical Framework is the conceptual framework used for this study [31;32]. Its core elements are consistent with FIPs, and, like FIPs, it aims to mitigate privacy risk [31;32]. The Framework has previously been validated examining the use of personal information in integrated information technology environments, i.e., the Internet. It is based on six core privacy dimensions that include: *control* over personal information, *collection* of personal information, *transparency/awareness* of privacy rights and organizational privacy practices, *preventing unauthorized access*, *authorization for health research* and the influence of these dimensions on trust and risk beliefs (and ultimately releasing personal health information) [31;32]. The dimension concerning authorization for health research is of particular interest in this study. In the Framework, this dimension is concerned with obtaining adequate consent and/or authorization for health research (secondary uses) as well as utilizing safeguards as a way of mitigating the risk of privacy breaches while enhancing public trust [31;32]. With single discrete studies expanding into prospective disease or treatment-based databases without clear research questions, and the expected large scale demand of secondary uses of PHI from electronic health records, numerous challenges to PHI protection including obtaining consent and safeguarding data exist [7;33-35].

## Methods

The research proceeds through five phases, leading to both qualitative exploration and quantitative content analysis of relevant documents available in the public domain. More specifically:

1) A review of the literature and a general Internet search using the Google search engine provide an updated compellation of international FIPs [9;42;43]. The Google search terms include: "fair information principles" and "practices" AND "FIPS", AND "Canada", "European Union", "Europe", "United States", as well as the "Middle East" and other continents including "Africa", "South America" and "Asia-Pacific". Additional search terms used are: "fair information principles" AND "privacy legislation", AND "privacy statutes".

***Inclusion/exclusion criteria: FIP selection***

Inclusion criteria included that the FIPs are recognized within their jurisdiction and have been used to guide the development of privacy legislation. The FIPs were limited to those presented in English or French. In this study, no FIPs that were identified in the search were excluded. All documents were then extracted and tabulated in terms of the principle or standard identified within the Canadian context (showing direct similarities and differences).

2a) In order to identify health research privacy policy and guidance documents that are used internationally for health research, the following search terms were used in the Google search engine: health; medical research; biomedical research; privacy; practices; principles AND (countries/continents listed above) AND international organizations that are known to offer guidance such as World Health Organization (WHO); Council for International Organizations of Medical Sciences (CIOMS); World Medical Association( WMA); and United Nations (UN). Policy documents were defined as those that are requirements in their respective jurisdictions, while guidance documents are optional.

***Inclusion/exclusion criteria: document selection***

Public domain documents are the focus throughout this study as it is the intent of this work to identify, review, analyze and synthesize documents that are broadly known to either the privacy or health research communities and that are related to information privacy protection in health research. Only documents that were either in English or French were included. Searches were replicated by a research assistant (PM). Documents were searched from an unspecified start date to January 1, 2013. All phases of this project began with online queries

using the search engine Google. Branching to links or document references/citations followed.

This study excludes any health guidance documents that did not include or reference privacy or that did not focus on health research, or conversely focused exclusively on specific areas of activity. For example, guidance documents exclusively dedicated to genetics, HIV/AIDS (or other specific conditions), health/disease registries, health surveillance databases, particular populations and human biological material were considered out of scope for this research.

Content analysis of health research guidance documents was then conducted and tabulated according to the following characteristics:

i. Whether the documents were specific to the protection of PHI or broader health research practices in general;
ii. Whether broader ethics principles or FIPs (or both) provided overarching structure.

2b) In order to have a systematic method of comparison of the international privacy guidance document with those in Canada, the two Canadian health research documents, i.e., the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans [TCPS 2] and the CIHR Best Practices for Protecting Privacy [CIHR BPPP]), had their practice guidelines itemized by the researcher.

As the CIHR BPPP was subjectively observed to contain more guideline items than the TCPS 2, it was itemized first. The content of the CIHR BPPP lists were then verified by a research assistant (PM) and a member of the CIHR Privacy Advisory Committee (JH). The TCPS 2 document was subsequently compared to this list of validated items; similar practices were extracted and any additional ones were added to create a catalogue listing of all TCPS 2 privacy practices. The TCPS 2 list, however, was not externally verified. Any privacy practices related to specific populations, human biological materials, genetic research or clinical trials were excluded as they were out of scope for this study.

The two lists of practices were merged into one "combined" or "master" list for ease of analysis. It is, however, clear which items belong to which documents. This "master list" provided a systematic way of examining harmonization between the Canadian documents and allowed for a comparison to the international community. It should be noted that in its current form, the "master list" is not intended as an indicator of document quality, i.e., more items does not imply a "better" document. Nor does it suggest "a list of things to be checked off" by researchers or ethics review boards. The resulting list serves only as a template for systematic comparison. Data management for the item-by-item comparison between the "master list" containing the CIHR BPPP and TCPS 2 items with the international context was done using the Microsoft Excel program.

c) The international documents were examined item-by-item to identify additional practice guideline items. For ease of analysis, items were grouped according to the CSA Model Code 10 privacy principles (as adapted by CIHR for health research) [38]. As such, the 10 principles have been rearranged and regrouped as follows: 1) Determining research objectives; 2) Limiting collection of personal information data; 3) Consent requirements; 4) Managing consent; 5) Informing prospective participants about the research through informed consent ; 6) Recruiting participants; 7) Safeguarding personal data; 8) Controlling access; 9) Retention of data; and 10) Accountability and transparence [38]. Any *additional* items that did not fit into any of the 10 principles, would be listed and analyzed separately.

## Findings

### *Comparative analysis of international FIPs with the CSA Model Code 10 Privacy Principles*

The term "Fair Information Principles - FIPS" reportedly originates from previous guiding codes of practices that had broad national and international implications, specifically the "Code of Fair Labor Practices" [39]. A review of the literature indicates that the concept of FIPs appears to have first emerged in the United States in the early 1970s, over mounting concerns about computerized databases [9;37;40;41]. At approximately the same time, the Council of Europe was examining similar issues [9;37;40;41].

According to legal scholars, FIPs are the building blocks of modern information privacy law around the world and are foundational in the development of important international guidelines for privacy protection [9;36;37;40;42]. Currently, the vast majority of nations around the globe protect privacy in their constitutions [31]. **Figure 4-1** shows the development of FIPs and their impact on the legislative processes around the globe.

Differences in FIPs are minimal but do exist. For example, while all the OECD-derived FIPs and those from APEC provide an explicit collection limitation principle [9;37;40;43-51], the principle of openness or transparency is explicit only in the OECD Guidelines, and the EU data protection directive [37;40;45;46]. In The APEC Privacy Framework, transparency and openness are implied in the notice principle. As well, the EU directive and the APEC Privacy Framework introduce entirely new principles including: restrictions on onward transfers of data; special protection for sensitive data; limits on automated decision-making; and prevention of harm [37;40;45]. The differences in terminology are noted, e.g., collection limitation versus purpose specification versus use limitation, as well as the varying levels of abstraction [37;40;41;43;45]. Almost all FIPs including the OECD Guidelines (and their resulting Model Codes/standards) and the APEC Privacy Framework have explicit recognition of the need for proportionality and balance [37;40-46].

**Figure 4-1**

**The Evolution of Core Fair Information Practice Principles and their impact on International Privacy and Data Security Statutes**

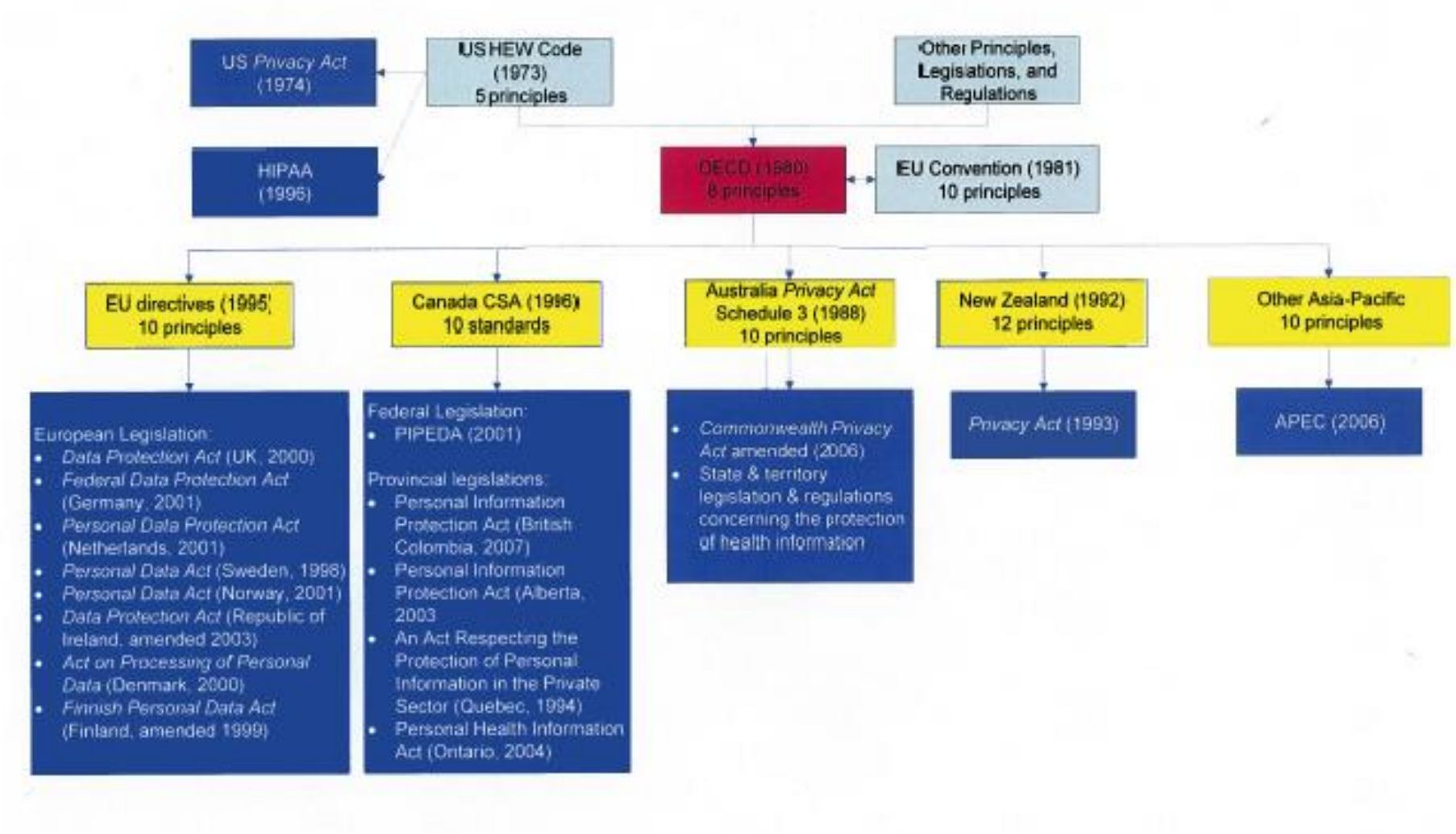


**Table 4-1** compares six frequently cited FIPs against those used in Canada (the CSA Model Code) and shows that they all share a common emphasis on empowering individuals to control their personal information, as opposed to merely protecting individuals from unfair or harmful uses of personal information [37;40;41;43;46]. All of the FIPs in the table reflect the same approach in terms of a data custodian's responsibilities: telling individuals what data will be collected or used; providing choice as to whether an individual wishes to provide data; granting access; securing data with appropriate technologies and procedures; and being subject to third-party enforcement for failure to comply [37;40;41;43;46].

As many FIPs are derived from the OECD Guidelines, they provide core commonalities for privacy protection. These commonalities are reflected in numerous legislative statues and standards in North America, Europe, and Asia and in many countries around the globe. Based on the above, they provide - in theory - a framework for harmonization in health research.

## Table 4-1

## Comparison of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information with International Fair Information Principles (FIPs)

| | CSA Model Code 10 Principles (1996) | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name/Source/Date | Principle #1 Accountability | Principle #2 Identifying Purposes | Principle #3 Consent | Principle #4 Limiting Collection | Principle #5 Limiting use, disclosure, and retention | Principle #6 Accuracy | Principle #7 Safeguards | Principle #8 Openness | Principle #9 Individual Access | Principle #10 Challenging Compliance | Additional Principles #11 Enforcement | Additional Principles #12 Transborder Data Flows | Additional Principles #13 Sensitive Data | Other Additional Principles |
| Fair Information Practices **Source:** US Dept. of Health, Education and Welfare (HEW) **Date:**1973 | | | | Collection limitation | Secondary Use | Record Collection | Security | | Disclosure | | | | | |
| Privacy Guidelines **Source:** OECD **Date:** 1980 | Accountability Principle | Purpose Specification | Use Limitation Principle | Collection limitation | Use Limitation Principle | Data Quality Principle | Security Safeguards Principle | Openess Principle | Individual Participation Principle | Individual Participation Principle | | Transborder Data Flows | | |
| Convention for the Protection of Indivuals with regard to Automatic Processing of Personal Data **Source:** Council of Europe **Date:** 1981 | | Quality of Data (b) | | Quality of Data (c) | Quality of Data (b)(e) | Quality of Data (d) | Data Security | Additional safeguards for the data subject | Additional safeguards for the data subject | Additional safeguards for the data subject | Sanctions and Remedies | Transborder Data Flows | Special categories of Data | Assistance to data subjects abroad |
| National Privacy Principles **Source:** *Privacy Act* - Australia **Date:** 1988 | | Collection | | Collection | Use and Disclosure | Data Quality | Data Security | Openess | | | | Transborder data flows | Sensitive Information | Identifier<br>Anonymity |
| Information Privacy Principles **Source:** New Zealand **Date:** 1993 | | Purpose of collection of personal information | | Collection of Information | Personal information not to bekept longer then necessary<br>Limits on use of personal information<br>Limits on disclosure of personal information | Correction of personal information<br>Accuracy of personal information to be checked before use | Storage and security of personal information | | Access to personal information | | | | | Source of personal information<br>Manner of collection of personal information<br>Unique identifies |
| APEC Privacy Framework **Source:** APEC **Date:** 2006 | | Notice/Awareness | Choice/ Consent | | | Access/ Participation | Integrity/ Security | Notice/ Awareness | Access/ Participation | | Enforcement | | | Parental Notice |

**Table 4-1 (cont.)**

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | "explicitly specify the purpose" | | | | "maintain accuracy" | "protect the securty of personal information" | "infuse transparency" | | | | | | "gather information by lawful and appropriate means" |
| | Notice | Choice | Data Integrity | | Data Integrity | Security | Notice | Access | | Enforcement | | | |
| Accountability | | Choice | Collection limitation | Uses of Personal Information | Integrity of Personal Information | Security Safeguards | Notice | Access and Correction | | | Due Diligence in Transfers | | Preventing Harm |

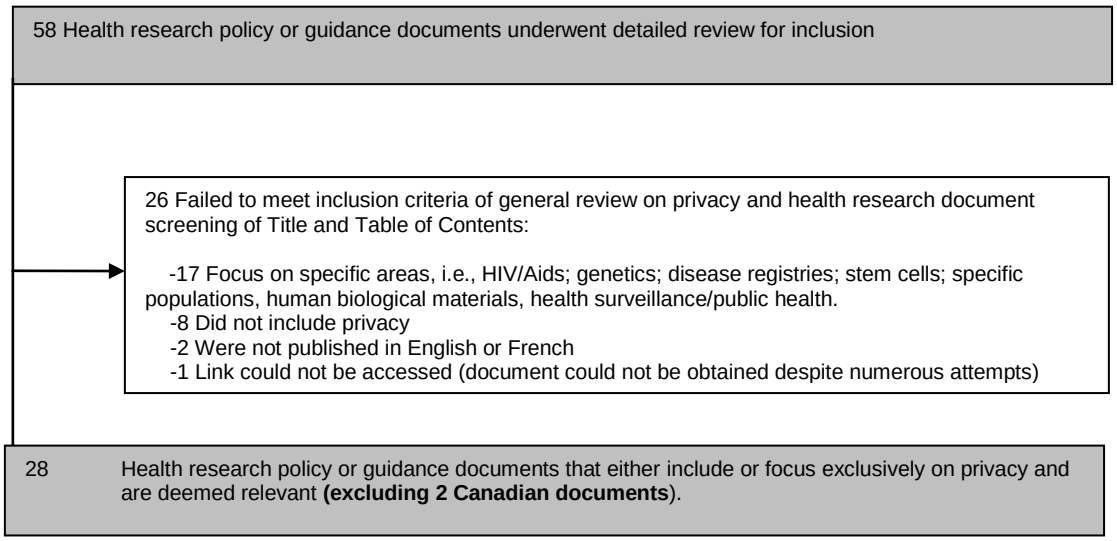
***Canadian policy and guidance documents***

In Canada, the two principle health research and privacy policy and guidance documents, TCPS 2 and the CIHR BPPP, are based on FIPs as outlined in the CSA Model Code [38;47;48].

The TCPS 2 is the most influential Canadian policy applicable to the ethics of research with human participants and widely followed by Canadian researchers and institutions including Canadian research ethics boards (REBs) [48]. The CIHR BPPP, on the other hand, is a guidance document [38]. Its use in the Canadian context is optional, however, as a document dedicated only to privacy protection in health research, it presents the most detail in terms of listing possible privacy practices; it comprises a total of 158 privacy risk mitigating considerations (**Appendix 1**). The TCPS 2 includes a total of 106 privacy specific items. This list of 106 items includes four additional items that are not found in the CIHR BPPP. The four additional practices, which include two related to obtaining ongoing consent from participants and two identifying secondary use scenarios excluded from REB review, were added to the 158 items of the CIHR BPPPs list to create a combined listing of 162 privacy practices (**Appendix 1)**[48]. This results in a "combined list" of 162 unique practices.

The search of international documents that direct privacy practices in health research identified 28 documents, not including the two Canadian documents (**Figure 4-2**). With the Canadian documents used as the comparator, a content analysis of international research guidance documents reveals which documents are: a) privacy specific; or b) embedded within broader ethics principles; and/or c) reference FIPs.

**Figure 4-2: Flow chart for the selection of international privacy health research policy and guidance documents**




The five of 28 (18%) documents that were derived from both ethics principles and FIPs or FIPs alone, and were specific to health research privacy, show the greatest commonalities with the Canadian documents (**Table 4-2**). The two EU documents based on FIPs compare minimally with the Canadian context. Twenty one of 28 (75%) documents do not reference FIPs at all, and share less than 55% (mean 30%) of practices with TCPS 2 and less than 45% (mean 26%) of CIHR BPPP practices (**Table 4-2**).

Documents emerging from the United Kingdom show the greatest similarity with the CIHR & TCPS documents, followed by Singapore, the United States and CIOMS. While few documents share the large number of TCPS 2 or CIHR BPPP practice items, 86% of the documents (24 of 28) have at least 70% of their privacy practice items in common with both TCPS 2 and CIHR BPPP.

**Table 4-2: Overall Comparative Analysis of International Guidance Documents with CIHR BPPP and TCPS 2**

yellow= Canadian documents
white=International documents

| | *Privacy Specific | *Based On Ethics | *Based on FIPs | *Secondary Use Guidance | *Database (multiple purpose) Guidance | **CIHR BPPP 158 items | **TCPS 2 106 items |
|---|---|---|---|---|---|---|---|
| **CIHR BPPP 158 items** | √ | √ | √ | √ | √ | | 101/106 |
| **TCPS2 106 items** | | √ | √ | √ | √ | 101/158 | |
| **International Health Research Guidance Documents Total n=28 documents** | **Privacy Specific (√) n=7** | ***Based On Ethics (√) n=23** | ***Based on FIPs (√) n=7** | ***Secondary Use Guidance (√) n=18** | ***Database (multiple purpose) Guidance (√) n=11** | ****CIHR BPPP 158 items** | ****TCPS 2 106 items** |
| **1) Personal Information in Medical Research 2000; 2003) (PIMR-UK) 123 items** | √ | √ | √ | √ | √ | 1) 101/158 (64%) 2) 101/123 (82%) | 1) 77/106 (73%) 2) 77/123 (63%) |

| | *Privacy Specific | *Based On Ethics | *Based on FIPs | *Secondary Use Guidance | *Database (multiple purpose) Guidance | **CIHR BPPP<br>158 items | **TCPS 2<br>106 items |
|---|---|---|---|---|---|---|---|
| **2) Integrated Research Application System (2009)**<br>**(IRAS-UK)**<br>**97 items** | | √ | √ | √ | √ | 1) 86/158 (54%)<br>2) 86/97 (89%) | 1) 67/106 (63%)<br>2) 67/97 (70%) |
| **3) Towards Consensus for Best Practice: Use of patient records from general practice for research (2009)**<br>**(TCBP-UK)**<br>**84 items** | √ | √ | √ | √ | √ | 1) 76/158 (48%)<br>2) 76/84 (90%) | 1) 69/106 (64%)<br>2) 69/84 (82%) |
| **4) Personal Information in Biomedical Research (2007)**<br>**(PIBR-Sing)**<br>**90 items** | √ | √ | √ | √ | √ | 1) 74/158 (47%)<br>2) 74/90 (82%) | 1) 62/106 (59%)<br>2) 62/90 (69%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **5) Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule (2004)**<br>**(HIPPA-US)**<br>**80 items** | √ | | √ | √ | √ | 1) 58/106 (55%)<br>2) 58/80 (73%) | 1) 71/158 (45%)<br>2) 71/80 (89%) |
| **6) International Ethical Guidelines for Epidemiological Studies (2009)**<br>**(EPI-CIOMS)**<br>**71 items** | | √ | | √ | √ | 1) 57/106 (54%)<br>2) 57/71 (80%) | 1) 70/158 (44%)<br>2) 70/71 (99%) |
| **7) Guidelines on Ethics in Health Research (2002;2005)**<br>**(GEHR-NZ)**<br>**60 items** | | √ | | √ | √ | 1) 53/106 (50%)<br>2) 53/60 (89%) | 1) 60/158 (40%)<br>2) 60/60 (100%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **8) Ethical Guidelines for Observational Studies: Observational Research, Audits and Related Activities (2012) (EGOS-NZ)** **67 items** | | √ | | √ | √ | 1) 53/106 (50%) 2) 53/67 (79%) | 1) 59/158 (37%) 2)59/67 (89%) |
| **9) Handbook For Good Clinical Research Practice (GCP)(2002)(GCP-WHO)** **64 items** | | √ | | √ | | 1) 53/106 (50%) 2) 53/64 (83%) | 1) 60/158 (38%) 2) 60/64 (94%) |
| **10) International Ethical Guidelines for Biomedical Research Involving Human Subjects (2002) (BMHS-CIOMS)** **60 items** | | √ | | √ | √ | 1) 36/106 (34%) 2) 36/60 (60%) | 1) 58 /158 (38%) 2) 58 /60 (97%) |
| **11) Guidelines on Ethics For Medical Research: General Principles (2002) (GEMR-SA)** **77 items** | | √ | | √ | | 1) 52/106 (49%) 2) 52/77 (68%) | 1) 57/158 (36%) 2) 57/77 (74%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **12) European Union Directives e Privacy (ePriv-EU)**<br>**54 items** | √ | | √ | √ | √ | 1) 49/106 (46%)<br>2) 49/ 54 (91%) | 1) 53/158 (34%)<br>2) 53/54 (99%) |
| **13) National Statement on Ethical Conduct in Human Research (2007) (NECHR-Aus)**<br>**54 items** | | √ | | | | 1) 45/106 (42%)<br>2) 45/54 (83%) | 1) 48/158 (30%)<br>2) 48/54 (89%) |
| **14) Interim Good Clinical Research Practice Guidelines: Volume 3 (1998) (IGCRP-NZ)**<br>**47 items** | | √ | | √ | | 1) 45/106 (42%)<br>2) 45/47 (96%) | 1) 47/158 (30%)<br>2) 47/47 (100%) |
| **15) Personal Data for Public Good: Using Health Information in Medical Research (2006) (PDPG-UK)**<br>**47 items** | √ | | | √ | | 1) 42/106 (40%)<br>2) 42/47 (89%) | 1) 47/158 (30%)<br>2) 47/47 (100%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **16) Ethics in Health Research: Principles, Structures and Processes (2004) (EHRSP-SA)**<br>**44 items** | | √ | | √ | | 1) 42/106 (40%)<br>2) 42/44 (95%) | 1) 44/158 (28%)<br>2) 44/44 (100%) |
| **17) Ethical Guidelines on Research Involving Human Subjects (1997) (EG-SING)**<br>**40 items** | | √ | | | | 1) 34/106 (32%)<br>2) 34/40 (85%) | 1) 40/158 (25%)<br>2) 40/40 (100%) |
| **18) E6 Good Clinical Practice: Consolidated Guidance (1996) (ICH)**<br>**36 items** | | √ | | | | 1) 31/106 (29%)<br>2) 31/36 (86%) | 1) 35/158 (22%)<br>2) 35/36 (97%) |
| **19) European Union Directive 95/46**<br>**(1995) (EU 95/46)**<br>**35 items** | √ | | √ | √ | √ | 1) 31/106 (29%)<br>2) 31/35 (89%) | 1) 33/158 (21%)<br>2) 34/35 (97%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **20) Research Involving Human Subjects: Guidelines for IRBs - Annex IV/D (2004) (RIHS-SING)-**<br>**32 items** | | √ | | √ | | 1) 30/106 (28%)<br>2) 30/32 (94%) | 1) 32/158 (20%)<br>2) 32/32 (100%) |
| **21) WMA Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects (adopted 1964:last amended 2008) (WMA)**<br>**31 items** | | √ | | √ | | 1) 130/106 (28%)<br>2) 30/31 (97%) | 1) 31/158 (20%)<br>2) 31/31 (100%) |
| **22) Good Clinical Practices: Document for the Americas (2005) (PAHO-PA)**<br>**31 items** | | √ | | | | 1) 29/106 (27%)<br>2) 29/31 (94%) | 1) 31/158 (20%)<br>2) 31/31 (100%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **23) Operational Guidelines for Ethics Committees that Review Biomedical Research (2000) (OGE-WHO)** **31 items** | | √ | | | | 1) 27/106 (25%) 2) 27/31 (87%) | 1) 31/158 (20%) 2) 31/31 (100%) |
| **24) A Practical Guide For Health Research (2004) (PGH-WHO)** **29 items** | | √ | | | | 1) 27/106 (25%) 2) 27/29 (93%) | 1) 27/158 (17%) 2) 27/29 (93%) |
| **25) Australian Code for the Responsible Conduct of Research (2007) (CRCR-Aus)** **25 items** | | √ | | | | 1) 18/106 (17%) 2) 18/25 (72%) | 1) 24/158 (15%) 2) 24/25 (96%) |
| **26) Universal Declaration on Bioethics and Human Rights (2005)** **(UNESCO)** **17 items** | | √ | | | | 1) 13/106 (12%) 2) 13/17 (77%) | 1) 14/158 (9%) 2) 14/17 (82%) |

| Health Research Guidelines N=28 | Privacy Specific N=7 | Based On Ethics N=23 | Based on FIPs N=7 | Secondary Use Guidance N=18 | Database (multiple purpose) Guidance N=11 | TCPS 2 (106 items) | CIHR BPPP (158 items) |
|---|---|---|---|---|---|---|---|
| **27) Guidelines on the Practice of Ethics Committees in Medical Research with Human Participants: Fourth Edition (2007) (ECMR-UK)** **17 items** | | √ | | | | 1) 14/106 (13%) 2) 14/17 (82%) | 1) 17/158 (11%) 2) 17/17 (100%) |
| **28) Good Research Practice: MRC Ethics Series (2012) (GRP-UK)** **15 items** | | | | | | 1) 11/106 (10%) 2) 11/15 (73%) | 1) 12/158 (8%) 2) 12/15 (80%) |

*Documents that contained the criteria indicated at the top of the column were marked with an '√'. Those that did not contain the criteria were left blank. The number of '√' are identified at the top of each column, i.e., n=7 privacy specific documents.

**The same statistic is reported in two ways in both the TCPS2 and CIHR BPPP columns : 1) The percentage of similar items between the international document and either TCPS2 or CIHR BPPP, and 2) The percent of the international document that is made up of items similar to TCPS 2 and CIHR BPPP items.

***Comparative analysis of primary and secondary uses of PHI and guidance related to the creation of databases for general research purposes***

All of the documents referred to primary collections of PHI for health research first and foremost. In terms of which documents also provide specific guidance regarding secondary uses, 18 of 28 (64%) do so, while 11 of 28 (39%) provide privacy practices for general use databases. Of note, only one international document from the UK (*Towards Consensus for Best Practice: Use of patient records from general practice for research, 2009*) made reference to secondary uses of data collected specifically from EHRs. The remaining documents (including the ones from Canada) focused only on secondary uses of data in general.

All of the documents that were based on FIPs (alone or with ethics principles) include practices for both general secondary use activities as well as general use databases (**Table 4-2**).

In terms of specific secondary use practices, the18 documents that include these activities provide a provision requesting a waiver of consent in the processing of PHI. If the waiver is to be applied, 14 of 18 (78%) documents require that the risk of harm to participants be identified along with the research benefits so that the ratio of harm to benefits can be determined; this indicates that obtaining individual consent must be deemed impracticable, and adequate security measures must be in place. In many cases including Canada, the European Union, the United Kingdom, the United States, New Zealand and Australia, the exact requirements for permitting research without consent were found in the nation's legislation [32;46;50-55]. Regarding the creation of databases for general use purposes, six of 10 (60%) state that participants should be informed of the type of studies that might be conducted, as well as be given a method for controlling future uses of data, such as withdrawing consent at any time. Notably, these practices are generally consistent with the Canadian context.

***Comparative analysis of items not included in the Canadian documents (CIHR BPPP or TCPS 2)***

A total of 119 additional or innovative items are identified in the 28 international documents that are not present in either of the Canadian documents. As the analysis was conducted by comparing documents, duplicate items between documents were retained for analysis purposes. From this total, 19 items are duplicates, resulting in 100 additional items which are listed in **Table 4-3**. From this table, it should be noted that at least four items could be considered in conflict or disagreement with the Canadian documents, i.e., items 53, 61, 78 and 82. Fifteen items could be classified as "new", while the remaining 81 provided further specifications or variations to those found in either the TCPS 2 or CIHR BPPP.

Of the 119 total document items, 102 can be classified according to the 10 adapted CSA core principles. Notably, the majority of additional items in this grouping of 102, (62 of 102; 61%) can classify as either Principle 5, 7 or 2 (**Table 4-4)**.

In *Principle 5: Informing prospective participants about the research through informed consent,* 32 of 102 (31%) additional items are recognized. As part of consent, *Principle 5* focuses on what should be included in the consent process, that is, information about the nature of the research, what information is collected, how it is used in this study and possible future studies, as well as the risks and benefits of the research [38]. Hence, these additional items focus on further developing Principle 5. Guidance documents, particularly from Australia, New Zealand and South America, clearly speak to the importance of taking additional measures to ensure that research participants truly understand to what they are consenting. Furthermore, New Zealand and Australia indicate that if the data (including that deemed anonymous) is to be used for secondary purposes, the subject should be informed beforehand. South Africa proposes the use of scientists or physicians who are independent of the study be available to the research subjects during the consent process in order to answer questions and clarify outstanding matters. Finally, Singapore highlights the importance of customizing consent forms as much as possible to the subject's capacity.

The next largest grouping of additional items, 19 of 102 (19%), is in *Principle 7: Safeguards*. Findings show that in the UK, EU, South Africa, Singapore and New Zealand, the importance of breach protocols being in place, along with breach notification to research subjects, figures prominently for managing and protecting electronic data.

**Table 4-3: Summary- Additional/Variation International Privacy Practices List (n=100 items) (with 19 duplicates removed)**

1. Identify requirements for data to be deemed truly de-identified, i.e., anonymous.
2. Identify requirements for obtaining certification that data is truly de-identified, i.e., anonymous.
3. Consent forms must be specific to a present research study and should include potential uses and disclosures of PHI.
4. Consent forms must provide information on all collected elements and their purpose and uses. Forms must also inform individual of their right to withdraw at any point and the specific expiration point for their consent, i.e., end of study.
5. Identify the elements to be removed from data to create a limited data set which may be used without obtaining individual consent.
6. Identify the elements required for a data use agreement authorizing the use and disclosure of a limited data set.
7. Identify all individuals who will have access to personal health information for purposes preparatory to proposed research.
8. Describe procedures in place to document all disclosures of PHI (this should include the date the disclosure was made, the name and address of the recipient of the PHI, a description of the PHI disclosed, and the reason for the disclosure).
9. Participants will be able to access their personal health information at any time or location which is convenient to them.
10. To individuals: written notice of researcher's privacy practices and individual's privacy rights are provided to the participant.
11. Acknowledging that few data can be considered truly anonymous, identify privacy protections for handling anonymized data.
12. Identify organizations considered "Honest Brokers" for conducting data linkage activities and data quality checks.
13. Describe mechanisms for accreditation and accountability.
14. Outline potential sanctions in place for breach of confidentiality.
15. Demonstrate that procedures are in place for identifying, reporting, and responding to lapses in good practices.
16. Recruitment: Prospective participants should be allowed to opt-out.
17. Identify the steps taken to modify data to ensure those who view it are unaware of individual identities, i.e., anonymized (linked or unlinked), coded, etc.
18. Identify extra precautions taking in handling sensitive data, i.e., information relating to mental health, sexuality, etc.

19. List all individual(s) responsible for the removal or coding of identifying information and their relationship to the team or organization responsible for the participant's care.
20. Technical security measures including: transferring any identifiable personal data from a portable device to a secure computer and the earliest opportunity and removing data from portable device's memory.
21. Technical security measures including:
    a. Displaying a confidentiality warning message to all users entering an electronic system on which personal information is stored.
    b. Ensuring users check, at log-off, to ensure all documents containing confidential information cleared from any applications available at computer start-up.
    c. Minimizing personal medical information transmitting electronically and using an appropriate level of encryption when electronic transmission is unavoidable.
22. Identify individuals responsible for:
    a. Overall management and control of research data.
    b. Responding to breaches of security or leaks.
    c. Maintaining a backup and disaster recovery process.
    d. Controlling file access rights and duplications.
23. Describe process for ensuring data security or disposal after project completion.
24. Identify process for mitigating potential harm to participants that may stem from research activities.
25. Will published data include potential identifiers which could reveal participant's identity to close relatives or friends?
26. For research about small groups of people, indicate steps taken to prevent re-identification when publishing results.
27. Study information and consent forms should include notice that information in one study may be used in anonymized form for another study.
28. Specify custodian of the data in the event that the research group conducting the study dissolves.
29. Consent process: Inform participant of any expected secondary uses (including: potential impact on their interests, a contact person for these secondary uses, and what types of information may be passed on).
30. Specify risk proposed use(s) of data could present to patient trust in health professionals.
31. Identify standards for data transfer including use of diagnostic or treatment codes, and methods for quality control.
32. Recruitment: Identify any research nurses involved in participant recruitment.

33. Recruitment: identify individual (a doctor independent from the subjects) to review records for selection.
34. Will provided funding be sufficient to ensure research is done well, safely, and ethically?
35. Organizational safeguards: researchers leaving the establishment should only be allowed to retain data/copies of data with permission from their team leader or department head, and only if it is clear that the future use of personal information will be consistent with terms of consent.
36. Identify storage and security processes for signed consent forms.
37. Identify all data processing activities involving the sharing of personal data, the viewing of collected data by individuals outside the care team, the publishing of personal data, i.e. direct quotations.
38. Ensure full knowledge of security procedures is shared only with those authorized to access data.
39. Outline confidentiality policies, confidentiality clauses in staff contracts, and measures undertaken to ensure staff awareness of confidentiality standards.
40. Clearly identify the specific risks/benefits of participation and non-participation.
41. Describe any existing relationship between the "recruiter" and the patients targeted for recruitment.
42. Outline process for determining if participants are capable of giving informed consent.
43. Outline the process for handling the information of a participant who has lost the capacity to consent.
44. Identify extent to which data will be de-identified, i.e., identifiable, de-identified, reversibly de-identified, irreversibly de-identified.
45. Irreversibly de-identified data is exempt from privacy and confidentiality requirements.
46. Justify that the level of de-identification proposed for data is in proportion to the sensitivity of the collected information.
47. Justify that the amount of information provided to participants in the consent process is adequate for the level of risk and potential of harm inherent in the project.
48. Justify that proposed level of security is commensurate to potential risk of harm to research participants.
49. Consent process is adjusted on a case-by-case basis to ensure it is appropriate to each participant.
50. Participants are informed of process for ensuring security and confidentiality of data.
51. General consent is adequate for unspecified research.
52. With general consent data may be used for new studies without re-contacting participants.
53. All secondary use of data to be reviewed by REBs.

54. Identify procedures for disclosing information.
55. Outline consent process, acknowledging that informed consent is ongoing throughout the study.
56. Consent can only be obtained from individual participants and not community leaders or other designated authorities.
57. Identify the manner and context in which informed consent is obtained from participants.
58. Identify potential impact of research may have on future generations.
59. Identify potential impact of research on surrounding environment.
60. Identify how process for disposing of records respects both the confidentiality of the participants and the broader community.
61. Consent process: Both written and verbal consent must be obtained.
62. Consent process: Information to participants must be clear, simple, and culturally appropriate manner.
63. Consent process: Environment for interaction should be non-threatening with peer counseling available.
64. Consent process: Participants must be informed of qualifications of research team.
65. It is preferable for data to be collected in de-identified form.
66. Precautions should be taken to maintain confidentiality of all data regardless of source.
67. All research records must have names of participants removed and replaced with codes.
68. The principle investigator retains responsibility for control list of names and codes, and maintaining confidentiality.
69. Identify process to keep identifiers separate from patient records.
70. Recruitment: Circulars, notices, and announcements to groups are preferable to individual approaches.
71. Recruitment: Recruitment should be conducted by an individual within potential participant's circle of care.
72. Identify process for obtaining consent for retrospective analyses.
73. Identify method for documenting informed consent, i.e., written, oral, audio-taped, video recorded.
74. Consent process: Participants should be informed of uses and privacy protections for their personal information in both coded and identifiable form.
75. Recruitment: Obtain patient consent prior to review of records.
76. Recruitment: Records used in prospective review must be de-identified and accessed only with REB approval.
77. Qualitative research: Where possible, verbal consent should be obtained to ensure greater anonymity of participants.

78. Qualitative research: Participants should receive some form of reciprocity for taking part in research.
79. Provide information on the backgrounds of the researchers, i.e., CVs, biographical sketch.
80. Justify that amount of data collected and retained is not excessive.
81. Identify process for involving community representatives in planning and conducting research.
82. Consent process: Consent from community representative may be acceptable when informed consent from all participants is not possible.
83. Justify chosen consent process when individual obtaining consent is neither the researcher nor a relevant health professional, i.e., participant's doctor.
84. Does the study comply with all relevant privacy legislation?
85. Outline process for ensuring consent is ongoing and that participant may withdraw at any time or from any portion of a study.
86. Consent forms must be provided in a preferred language of participant or an interpreter must be provided.
87. Consent forms must provide notice of relevant privacy legislation.
88. Consent forms must include information on all alternative treatment options.
89. Identify type of consent sought for future use, i.e., specific, extended, or unspecified.
90. Consent process: Participants should be given an oral or written test to assess informed consent.
91. Identify procedures in place to prevent disclosure of a participant's personal data to immediate family relatives without consent.
92. Data must be stored only to the extent necessary to complete service client consented to.
93. Data to be used for secondary uses should be anonymized.
94. Procedures must be in place to ensure clients can receive their results in anonymized format, i.e., non-itemized bills.
95. Consent requirements can be waived when it is proportionate to privacy risks and public interest benefits of research.
96. Demonstrate that confidentiality procedures reflect the risk research poses to public trust in health-care professionals.
97. Privacy procedures should be in proportion to risks involved in the proposed research.
98. Describe process for continuous reevaluation of anonymization process.
99. Justify individuals who will have access to data, i.e., need to know, individual obligation to data confidentiality.
100. Outline process for maintaining key for coded/anonymized data.

## Table 4-4: Additional Privacy Practice Items

**Additional Privacy Practice Items in Principle 5: Informing Participants**

| Source | Additional items: Informing Participants through Informed Consent |
|---|---|
| **HIPAA-US** | 1) Consent forms must provide information on all collected elements and their purpose and uses. Forms must also inform individual of their right to withdraw at any point and the specific expiration point for their consent, i.e., end of study.<br>2) Identify all individuals who will have access to personal health information for purposes preparatory to proposed research.<br>3) Participants will be able to access their personal health information at any time or location which is convenient to them.<br>4) Written notice of researcher's privacy practices and individual's privacy rights are provided to the participant. |
| **PIMR-UK** | 5) Study information and consent forms should include notice that information in one study may be used in anonymized form for another study.<br>6) Inform participant what happens to collected data upon completion of the study.<br>7) Inform participant of any expected secondary uses (including: potential impact on their interests, a contact person for these secondary uses, and what types of information may be passed on). |
| **PIBR-Sing** | 8) Justify that the amount of information provided to participants in the consent process is adequate for the level of risk and potential of harm inherent in the project.<br>9) Consent process is adjusted on a case-by-case basis to ensure it is appropriate to each participant. |
| **GCP-WHO** | 10) Identify the manner and context in which informed consent is obtained from participants. |
| **EHRSP-SA** | 11) Both written and verbal consent must be obtained.<br>12) Information to participants must be clear, simple, and culturally appropriate manner.<br>13) Environment for interaction should be non-threatening with peer counseling available. |

| Source | Additional items: Informing Participants through Informed Consent |
|---|---|
| **GEMR-SA** | 14) Identify method for documenting informed consent, i.e., written, oral, audio-taped, video recorded.<br>15) Participants should be informed of uses and privacy protections for their personal information in both coded and participants should receive some form of reciprocity for taking part in research.<br>16) Identify clinician external to both the project and the patient who will act as independent source of information and advice to potential participants. |
| **IGCRP-NZ** | 17) Identify process for obtaining consent in both written and oral form.<br>18) Outline process for ensuring consent is ongoing and that participant may withdraw at any time or from any portion of a study.<br>19) Consent forms must be provided in a preferred language of participant or an interpreter must be provided.<br>20) Consent must include information on all alternative treatment options.<br>21) Qualitative research: Where possible, verbal consent should be obtained to ensure greater anonymity of participants. |
| **ICH** | 22) Consent forms must include information on all alternative treatment options. |
| **EGOS-NZ** | 23) Identify process for involving community representatives in planning and conducting research.<br>24) To a reasonable extent, investigators should provide participant with information about individuals accessing study data.<br>25) Consent from community representative may be acceptable when informed consent from all participants is not possible.<br>26) Justify chosen consent process when individual obtaining consent is neither the researcher nor a relevant health professional, i.e., participant's doctor. |
| **NSECHR-Aus** | 27) Consent forms must note participants' right to withdraw at any stage and include implications of withdrawal and use of personal information after withdrawal.<br>28) Consent forms must include information on all alternative treatment options.<br>29) Identify type of consent sought for future use, i.e., specific, extended, or unspecified.<br>30) Outline process for ensuring consent is ongoing and that participant may withdraw at any time or from any portion of a study. |

| Source | Additional items: Informing Participants through Informed Consent |
|---|---|
| **IEG-CIOMS** | 31) Subjects are informed of their right to access data on demand or if access is not possible subjects are informed of the reason for non-disclosure.<br>32) Identify procedures in place to prevent disclosure of a participant's personal data to immediate family relatives without consent. |

**Additional Privacy Practice Items in Principle 7: Safeguards (not included in CIHR BPPP)**

| Document | Additional items: Safeguarding Personal Data |
|---|---|
| **PIMR-UK** | 1) In the event of a breach of confidentiality, identify the disciplinary consequences for the responsible individual(s).<br>2) Technical security measures including: transferring any identifiable personal data from a portable device to a secure computer and the earliest opportunity and removing data from portable device's memory.<br>3) Technical security measures including:<br>a) Displaying a confidentiality warning message to all users entering an electronic system on which personal information is stored.<br>b) Ensuring users check, at log-off, to ensure all documents containing confidential information cleared from any applications available at computer start-up.<br>c) Minimizing personal medical information transmitting electronically and using an appropriate level of encryption when electronic transmission is unavoidable. |
| **GRP-UK** | 4) Organizational safeguards: researchers leaving the establishment should only be allowed to retain data/copies of data with permission from their team leader or department head, and only if it is clear that the future use of personal information will be consistent with terms of consent.<br>5) Identify storage and security processes for signed consent forms. |

| | |
|---|---|
| **IRAS-UK** | 6) Ensure full knowledge of security procedures is shared only with those authorized to access data.<br>7) Identify storage and security processes for signed consent forms.<br>8) Outline confidentiality policies, confidentiality clauses in staff contracts, and measures undertaken to ensure staff awareness of confidentiality standards.<br>9) Identify where the collected data will be analyzed and the confidentiality safeguards used in its transfer.<br>10) Identify a procedure to response to a breach of confidence or failure to maintain data security.<br>11) Describe how the unexpected disclosure of information by individuals would be handled. |
| **GEMR-SA** | 12) Precautions should be taken to maintain confidentiality of all data regardless of source.<br>13) All research records must have names of participants removed and replaced with codes.<br>14) Identify steps required to ensure patient names remain confidential to person responsible for compilation.<br>15) Qualitative research: Identify process for ensuring anonymity of sensitive information. |
| **ePriv -EU** | 16) Procedures must be in place to inform clients when a breach of their confidentiality or privacy occurs. |
| **EGOS-NZ** | 17) Identify process for responding to breaches of privacy and confidentiality.<br>18) Identify process for informing participants of a breach of privacy or confidentiality. |
| **PIBR-Sing** | 19) Outline a privacy breach protocol. |

**Additional Privacy Practice Items in Principle 2: Limiting Collection (not included in CIHR BPPP)**

| Document | Additional items: Limiting Collection of Personal Data |
|---|---|
| **PIMR-UK** | 1) Identify the steps taken to modify data to ensure those who view it are unaware of individual identities, i.e., anonymized (linked or unlinked), coded, etc.<br>2) Identify extra precautions taking in handling sensitive data, i.e., information relating to mental health, sexuality, etc.<br>3) Identify process for mitigating potential harm to participants that may stem from research activities.<br>4) Specify risk proposed use(s) of data could present to patient trust in health professionals. |
| **PIBR-Sing** | 5) Identify extent to which data will be de-identified, i.e., identifiable, de-identified, reversibly de-identified, irreversibly de-identified.<br>6) Describe the extent to which personal information will be de-identified (as based on level of sensitivity).<br>7) Justify that the level of de-identification proposed for data is in proportion to the sensitivity of the collected information. |
| **EHRSP-SA** | 8) Identify extent to which data will be de-identified, i.e., identifiable, potentially identifiable, de-identified. |
| **PGHR-WHOEM** | 9) Justify that amount of data collected and retained is not excessive |
| **EGOS-NZ** | 10) Identify extent to which data will be de-identified, i.e., identifiable, potentially identifiable, de-identified. |
| **NSECHR-Aus** | 11) Identify extent to which data will be de-identified, i.e., identifiable, potentially identifiable, de-identified. |

Finally, 11 of 102 (11%) additional items classify as *Principle 2: Limiting Collection of personal information data elements.* Understandably, when dealing with electronic health information, limiting collection is a real concern. The concept of data de-identification through analytics or as a privacy enhancing technique is identified in health research privacy guidance documents in the UK, Australia, New Zealand, Singapore and South Africa, as they seek to identify strategies for minimizing the use of direct personal identifiers. In the UK, researchers are asked to clearly outline risks of harm to gain health-care provider and patient

trust, as part of the research review process and in particular when there is a collection of highly sensitive or large quantities of PHI.

**New groupings/elements**

Eleven of the 119 total items could not easily be grouped according to the 10 privacy principles. The three groupings/elements that emerged are outlined in **Table 4-5**.

**Table 4-5**

**New elements (groupings) not included in CIHR BPPP or TCPS 2**

| Element no. | Description | No. of items |
|---|---|---|
| **1** | **Identify requirements for data to be deemed "truly anonymous" and requirements for using or sharing such data.** | 7 |
| **2** | **Acknowledge difficulty in truly anonymizing data; identify privacy protection for anonymized data.** | 2 |
| **3** | **Demonstrate compliance with relevant privacy legislation and provide notice of said legislation to participants.** | 2 |

The first two elements focus on the concept of defining anonymous data. While this concept is linked to the principles of limiting collection as well safeguarding data, it is complex in that there are few guidelines on what "truly anonymous" data is. The first element attempts to provide guidance on anonymization requirements based on country specific contextual information that can influence de-identification risks, e.g., availability of voter registries in the United States. The second element examines the first concept in greater detail. It suggests that in this age where the risk of data re-identification is constantly increasing due to the proliferation of readily available databases, e.g., voting databases, and birth and death registries, creating a truly anonymized data set that is still useful is increasingly deemed unlikely [30;56;57].

Element 3 underscores the importance of identifying and complying with relevant privacy and data protection statutes by requiring demonstrated compliance in the documentation, and information regarding any relevant legislation is distributed to the participant. The items in

this category require that legal compliance be clearly outlined in consent forms that are reviewed and signed by research participants.

Element 4 (**Table 4-6**), is addressed in the TCPS 2, but is absent from CIHR BPPP. The international documents expand on the TCPS 2 with additional stipulations, such as requiring that procedures be in place when capacity to consent may become compromised during a study. This may be due to illness progression, treatment protocols or even death.

**Table 4-6: New elements (groupings)**
**not included in CIHR BPPP but referenced in TCPS 2**

| Element no. | Description | No. of items |
|---|---|---|
| **4** | **Outline procedures for determining individuals' capacity for consent and for responding to a loss of capacity to consent.** | 2 |
| **5** | **Describe how privacy protections are proportionate to potential risk(s) of research.** | 2 |

The fifth and final category highlights the need for proportionality when managing privacy risk. While this concept is stressed in the TCPS 2, it is implied in CIHR BPPP but not directly stated. Similar to other jurisdictions, TCPS provides few details on how to achieve this. Although presented as a separate category in this analysis, it is clear that proportionality is an overarching principle that by definition incorporates all of the items in a manner such that the more sensitive the PHI and the higher the risk of harm, the greater the need for more stringent privacy, confidentiality and security measures.

## Discussion

### *Chief findings*

As the Canadian policy and guidance documents are based on both FIPs and ethics principles, they show the highest number of similar privacy practice items with documents that are also based on these parameters. However, documents that were found to also be based FIPs represent 18% (five of 28) of all documents identified. Most of the documents did not utilize FIPs at all in the development of their privacy practices and instead based the practices according to ethics principles alone. At a time when other sectors such as finance, the private sector and government not only utilize FIPs, but are updating and revising FIPs and privacy legislation, the remaining documents have not kept up with today's technological developments [28-30]. Therefore, when it comes to privacy protection in health research, it is surprising that FIPs are not included in most international health research guidance documents [28-30].

However, the picture is relatively positive for Canada. For the vast majority of the International guidance documents, 86% (24 of 28), most of their listed privacy practices (70%) mirror those of the combined from the TCPS 2 and CIHR BPPP. This demonstrates that at a practice level, both the TCPS 2 and CIHR BPPP have a high degree of similarity with most international documents and additionally provide the Canadian health research community with comparatively more detail in terms of privacy risk mitigating practices.

Also on a positive note, even though they are not guided by FIPS, many international documents still attempt to address the challenging privacy issues that advancing technologies pose, including: secondary uses of data; creation of data repositories; data de-identification; and proportionality [38;48;50;53;55;58-66]. However, only one document mentioned the secondary uses of data from EHRs; despite the fact that EHR systems are being deployed globally.

In accordance with the Trust-Risk Theoretical Privacy Framework, the public's desire for adequate consent paired with data de-identification decreases perceived risk of privacy breaches and increases trust that personal information will be protected in health research

adhering to the TCPS2 and CIHR guidance [32;49;67]. However, the call for broader consent models for activities such as secondary uses of PHI, the increased engagement by researchers in the commercialization of the products of their research and the ever-increasing capability of technology to re-identify data previously believed to be anonymized, may have the reverse effect [68]. Results from this study show that globally, many jurisdictions share these concerns and have attempted to mitigate risks associated with these activities [38;48;50;55;58-66]. These privacy risk mitigating practices attempt to manage the new era of technological advances by tightening consent processes and requiring greater safeguards to manage the collection of ever larger quantities of data.

In terms of the additional practices (specifically the three "elements" or groupings) that emerged, show the international health research community's awareness that information privacy concerns require additional protections beyond basic safeguards and are consistent with those utilized in other sectors [28-30].

For example, the first two additional elements attempt to prevent the identification of subjects and violations of data protection when collecting, analyzing and disclosing data, by providing guidance (as in the US HIPAA Rule) related to data-de-identification or anonymization. In fact the HIPAA Rule is the only guidance that attempts to give clarity to t the concept of data de-identification. Analytics, which strips data of personal identifiers through the application of software technologies to data sets, has been gaining interest in many sectors such as finance, business and government for obvious reason [52-54]. While analytics provides a tool for data de-identification, many struggle with the question of when is de-identified data still personal information and when is it "truly anonymous" and not subject to privacy statues [56;68]. And others have argued that data is either ultimately identifiable and useful or "truly anonymous" and of little use, but never both [56;68]. The international health research community appears to be struggling along with other sectors to understand how analytics can best be used along with other privacy enhancing technologies to protect PHI but without giving a false sense of security to those using it [30].

This third element reveals the need to review different consent models, particularly for secondary collections, to ensure that they adequately meet the public's expectations but are also not overly restrictive to the research process [7;8;35]. In Canada, like many other countries, research ethics review boards can exempt observational studies from requiring consent on a case-by-case basis with the onus on the researcher to ensure that this is justified [50-55]. With emerging electronic health records in developed countries, the scale of secondary use of PHI is expected to increase substantially [7;33;51;52;55;69]. This has prompted some researchers to call for blanket exemption for observational research in order to minimize selection bias when obtaining individual consent, but this poses major logistical challenges [7;33;55;70]. Yet, in Canada, the public shows concern for confidentiality in these cases and requests some type of consent [7;33;49;55]. Further study is therefore required to understand the conditions under which the public would support using PHI without individual consent for both secondary uses as well as broad-based databases [7;33;49;55]. Interestingly, consent emerges again in the fourth element (unique to CIHR BPPP but not the TCPS 2), which places more responsibility on researchers by requiring them to anticipate and prevent against the loss of capacity to consent which may occur during the life cycle of the study.

In contrast, the fifth element, proportionality, offers a strategy for reducing the demands on researchers in terms of overly restrictive privacy practices. At the same time, it demonstrates to the public that appropriate privacy protection measures are in place. In Canada, while the TCPS 2 highlights the importance of proportionality: specifically, that privacy risk mitigating practices should be relative to the sensitivity of the PHI collected and the risk of harm. Neither the TCPS 2 nor any of the international documents guide REBs and researchers on how to accomplish this. Turning to other sectors may provide more detailed models for consideration. For example, the Government of Canada Security Policy classifies information (including personal information) as Protected A, B or C based on the type of harm (injury, serious injury, extremely grave injury) that could be expected if the information is compromised [71]. For each of the three classifications, specific security measures are outlined [71]. This model takes some of the guess-work out of determining privacy risk and how best to mitigate it. Proportionality provides additional privacy protection practices that

focus on the specific risk activities that need them. Thus, studies that pose minimal risk to privacy are not overburdened.

Of most significance is the fact that over 80% of the additional items simply provided further specifications or variations to those found in either the TCPS 2 or CIHR BPPP. This strengthens the point that the Canadian policy and guidance documents comparer well to international documents in terms of provisions offered for the protection of PHI in health research.

***Limitations of the research***

The collection of international guidance documents and their comparative analysis with the Canadian documents provides significant insight. However, as it was limited to document analysis, it did not include input from the documents' authors, health researchers or research ethics review boards. Interpretation of the documents was therefore left to the study author. Input from these key stakeholder groups would have provided interesting ideas regarding the guidance document usability and interpretation.

As this was a descriptive study, methodology and analysis were limited to meeting this objective. For example, one of the objectives of the study was to identify and create a list of new or innovative privacy practices. It can be argued that some of the list items are implicitly covered by either of the Canadian documents, and/or are not practical to implement, or that the items may be discussed in terms of proportionality. However, making judgment decisions about the appropriateness of items or development of a proportional classification of items is beyond the scope of this work.

As well, the Canadian and international documents themselves limit further in-depth analysis. For example, though a discussion of PHI in terms of different types of data, i.e., electronic health records, disease registries, administrative databases, would be of tremendous interest, the documents do not classify their privacy practices according to these headings. This type of discussion is therefore currently not possible. Finally, the TCPS 2 list of items does

benefit from verification by an independent party, as does the CIHR BPPP item list. This increases the risk of possible misclassification of items.

***Policy implications and directions for future research***

This study builds on previous work such as the 2001 CIHR document *Selected International Legal Norms on the Protection of Personal Information in Health Research*, and *Fair Information Practices and the Architecture of Privacy*. It not only provides a comprehensive, updated study of FIPs, but drills down to a practice-specific comparison which to the author's knowledge has not previously been done [9;36;37]. This gives ethics and privacy policy analysts a pragmatic understanding of how other jurisdictions address complex and emerging issues related to information privacy and health research and how the Canadian context compares. The findings from this work are particularly relevant given the increasing pace of international collaborative health research and the drive towards harmonization [9;36;37].

The 100 additional practices identified in international policy can be used (emulated, modified or avoided) in future revisions of Canadian policy and/or guidance documents to address current and emerging issues in a harmonized fashion. Important next steps might include having an expert panel reach a consensus about the list of 100 practices in terms of appropriateness and fit into the Canadian context, followed by classification and weighting of items into a proportional model. An expert panel using a Delphi approach could be one methodology that would allow both fit and proportionality to be addressed.

In terms of secondary uses of data, as well as the development of broad-based databases for health research, the findings from this study, along with previous works, suggest that there are no clear solutions regarding the waiver of consent models. However, without question, the public needs to be actively involved in these discussions [7;8;33;35].

## Conclusion

As both the TCPS 2 and CIHR BPPP documents are based on both FIPs and ethics principles, it can easily be said that they compare well to other international FIP-based policy and guidance documents, as well as to those that are based primarily on ethics principles. In fact, Canadian privacy protection practices include the majority of items from international documents and as such, are largely aligned with those in the international health research community. This is further confirmed by the fact that the vast majority of additional

guideline practice items are a variation (rather than being completely new) compared to those items found in either the TCPS 2 or CIHR BPPP.

However, the additional items (particularly the new groupings/elements) identified in this study may be considered in future revisions of both Canadian policy and guidance documents. This would promote an approach harmonized with the international community that would address the challenges faced with advances in information technology, with globalizing scientific research and with the public's desire for greater privacy protection.

## REFERENCES


(1) Implementation of the Data Protection Directive in Relation to Medical Research in Europe. Aldershot: Ashgate Publishing Limited; 2004.

(2) Institutes of Medicine. Protecting Data Privacy in Health Services Research. Washington D.C.: National Academy Press; 2009.

(3) Plomer A. *The Law and Ethics of Medical Research: International Bioethics and Human Rights*. New York: Routledge-Cavendish; 2005.

(4) Widdows H, Mullen C (Editors). *The Governance of Genetic Information: Who Decides*. Cambridge: Cambridge University Press; 2009.

(5) Burgess MM, O'Doherty K, Secko D. **Biobanking in British Columbia: discussions of the future of personalized medicine through deliberative public engagement**. *Personalized Medicine* 2008;**5**(3):285-96.

(6) Willison DJ, Kashavjee K, Nair K, Goldsmith C, Holbrook A. **Patient consent preferences for research uses of information in electronic medical records: Interview and survey data**. *British Medical Journal* 2003;**3**(26):373.

(7) Willison DJ, Swinton M, Schwartz L, Abelson J, Charles C, Northrup D. **Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public?** J AM Med Inform Assoc 2007; 14:706-12. doi 10.1197/jamia.M2457.

(8) Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM, **Computerization of Medical Practices for the Enhancement of Therapeutic Effectiveness investigators. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data**. *BMJ* 2003 Feb 15;**326**(7385):373.

(9) Canadian Institutes of Health Research (CIHR). Selected International Legal Norms on the Protection of Personal Information in Health Research. 2001.

(10) Bennett CJ, Raab CD. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: The MIT Press; 2006.

(11) Rozovsky LE, Inions. *Canadian Health Information* (3rd Edition). Butterworths, Ontario. 2002.

(12) EKOS Research Associates. Understanding Privacy and Security: Part of the Rethinking the Information Highway Study. 2003.

(13) EKOS Research Associates. Pan-Canadian Health Information Privacy and Confidentiality Framework Study. 2004.

(14) EKOS Research Associates Inc. Healthcare and the Internet: Part of the Rethinking the Information Highway Study. 2004.

(15) EKOS Research Associates Inc. Health Information and the Internet: Part of the Rethinking the Information Highway 2004/2005. 2005.

(16) EKOS Research Associates Inc. Revisiting the Privacy Landscape a Year Later. 2006.

(17) EKOS Research Associates Inc. Electronic Health Information and Privacy: What Canadians Think-2007. 2007.

(18) EKOS Research Associates Inc. Canadians and the Privacy Landscape. 2007.

(19) EKOS Research Associates Inc. Wave 2 Graphical Summary Report: Part of the Information Highway Study. 2007.

(20) EKOS Research Associates Inc. Wave 1 Graphical Summary Report: Part of the Information Highway Study. 2007.

(21) EKOS Research Associates Inc. Canadians and the Privacy Landscape. 2007.

(22) (COACH) Canadian Organization for Advancement of Computers in Health: Canada's Health Informatics Association. 2009 Guidelines for the Protection of Health Information. COACH; 2009.

(23) Bennett CJ. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: The MIT Press; 2008.

(24) Day B. **Why are doctors so concerned about protecting the confidentiality of patients records?** *Healthcare: Information Management & Communications Canada* 2008;**22**(N0.2):36-7.

(25) Institutes of Medicine. Protecting Data Privacy in Health Services Research. Washington D.C.: National Academy Press; 2009.

(26) World Medical Association (WMA). Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects. Seoul: 59th WMA General Assembly; 2008. Date accessed 06/03/2007. www.wma.net/en/30publications/10policies/b3/17c.pdf

(27) Solove DJ. *Understanding Privacy*. Cambridge: Harvard University Press; 2008.

(28) Kirby M. The history, achievement and future of the 1980 OECD guidelines on privacy. International Data Privacy Law 2010;3-11. Date accessed 17/10/2010. www.idpl.oxfordjournals.org

(29) Kuner C, Cate FH, Millard C, Svantesson DJB. Editorial. International Data Privacy Law 2010;1-2. Date accessed 17/10/2010. www.idpl.oxfordjournals.org

(30) Tene O. **Privacy: The new generation**. *International Data Privacy Law* 2010;12-9. Date accessed 17/10/2010. www.idpl.oxfordjournals.org

(31) Smith HJ, Milberg SJ, Burke SJ. **Information privacy: Measuring individuals' concerns about organizational practices**. *MIS Quarterly* 1996;**20**(2):167-96. www.jstor.org

(32) Malhorta NK, Kim SS, Agarwal J. **Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model**. *Information Systems Research* 2004;**15**(4):336-55.

(33) Willison DJ. **Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward**. *Journal of Health Services Research and Policy* 2003;**8**(1):S1:17-S1:23.

(34) Willison DJ. **Trends in collection, use and disclosure of personal information in contemporary health research: Challenges for research governance**. *Health Law Review* 2005;**13**(2&3):107-13.

(35) Willison DJ, Emerson C, Szala-Meneok K, Gibson E, Weisbaum K, Fournier F, et al. **Access to medical records for research purposes: Varying perceptions across Research Ethics Boards**. *Journal of Medical Ethics* 200 Apr;**34**(4):308-14. doi: 10.1136/jme.2006.0200328.

(36) Rotenberg M. **Fair information practices and the architecture of privacy: What Larry doesn't get"**. *Stan Tech L Rev* 2001;1-43.

(37) Gellman R. *Fair Information Practices: A Basic History*. Internet 2008 [cited 9 A.D. Nov 3];1-9. Date accessed 03/11/2009. http://bobgellman.com/rg-docs/rg-FIPshistory.pdf

(38) Canadian Institutes of Health Research. CIHR Best Practices for Protecting Privacy in Health Research. Ottawa: Public Works and Government Services Canada; 2005. Date accessed 20/05/2006. www.cihr-irsc.gc.ca/e/29072.html

(39) Ware WH. A Historical Note. 1993 p. 50. http://aspe.hhs.gov/pic/reports/ahrq/4441.pdf

(40) Cate FH. The Failure of Fair Information Practice Principles. Consumer Protection in the Age of the Information Economy (2006) 2006 [cited 9 A.D. Nov 3];343-377. Date accessed 03/11/2009. http://ssrp.com/abstract=1156972

(41) Council of Europe. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Council of Europe, European Treaty Series 1980 [cited 2007 Apr 15]; Council of Europe, European Treaty Series (No. 108). Date accessed 15/04/2007. www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt

(42) Schwartz PM. **Privacy and democracy in cyberspace**. *Vanderbilt Law Review* 1999;**52**:1607-14.

(43) Asia-Pacific Economic Cooperation. APEC Privacy Framework. 2004. Date accessed 28/07/2007. www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/ APEC+Privacy+Framework.pdf

(44) Canadian Standards Association. Canadian Standards Association (CSA) Model Code for Protecting Privacy. Canadian Standards Association 1996 [cited 2007 Mar 12]. Date accessed 12/03/2007. www.csa.ca/standards/privacy/code/Default.asp?language=english

(45) The Organization for Economic Cooperation and Development (OECD). The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Organization for Economic Cooperation and Development (OECD) 1980. Date accessed 04/08/2006. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

(46) Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 1995. http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

(47) Tri-Council Policy Statement : Ethical Conduct of Research Involving Humans, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (1998).

(48) Tri-Council Policy Statement : Ethical Conduct of Research Involving Humans - Second Edition, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (2012).

(49) Lysyk M., Graham I., El Emam K. **A decade of public trust: Canadians' opinion on privacy and electronic health information.** Electronic Healthcare, submitted 2013.

(50) Medical Research Council. Personal Information in Medical Research: MRC Ethics Series. London; 2000. Date accessed 25/07/2012. www.mrc.ac.uk/comsumption/idcplg?IdcService=GET_FILE&dID=6511&dDocName=MRC002415&allowInterrupt=1

(51) National Health and Medical Research Council, Australian Research Council, Universities Australia. Australian Code for the Responsible Conduct of Research. Australian Government; 2007.

(52) National Institutes of Health. Clinical Research and the HIPAA Privacy Rule. United States: U.S Department of Health and Human Services; 2004. Date accessed 17/09/2005. http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf

(53) National Research Ethics Service NPSAN. Integrated Research Application System (IRAS) - User's Manual. 2009. www.myresearchproject.org.uk/Help/Contents/IRASHelp_UserManual.pdf

(54) New Zealand Regulatory Guidelines for Medicines. Interim Good Clinical Research Practice Guidelines: Volume 3. 1998. www.hrc.govt.nz/assets/pdfs/publications/Ethics%20Guidelines%20July%202006.pdf

(55) Wellcome Trust. Towards Consensus For Best Practice: Use of patient records from general practice for research. London: Wellcome Trust; 2009. Date accessed 08/01/2009. www.wellcome.ac.uk/GPrecords

(56) Narayanan A, Shmatikov V. **Robust de-anonymization of large sparse datasets**. IEEE Symposium on Security and Privacy 2008.

(57) Sweeney L. *Uniqueness of simple demographics in the US population*. 2000. Carnegie Mellon University, Laboratory for International Data Privacy. Ref Type: Serial (Book, Monograph)

(58) Council for International Organizations of Medical Sciences (CIOMS). International Ethical Guidelines for Biomedical Research Involving Human Subjects. Geneva; 2002. Date accessed 27/07/2009. www.cioms.ch/frame_guidelines_nov_2002.htm

(59) International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals (ICH). Guidelines for Good Clinical Practice: ICH Harmonized Tripartite Guidelines E6. Published in the Federal Register; 1996. www.ich.org/LOB/media/MEDIA482.pdf

(60) Medical Research Council (MRC). Good Research Practice: MRC Ethics Series. London: Medical Research Council (MRC); 2000. Date accessed 27/07/2007. www.mrc.ac.uk/Utilities/Documentrecord/index.htm?d=MRC002452

(61) Medical Research Council of South Africa. Guidelines on Ethics For Medical Research: General Principles. South Africa; 2002. Date accessed 12/06/2010. www.kznhealth.gov.za/research/ethics1.pdf

(62) National Ethics Advisory Committee (NEAC). Ethical Guidelines for Observational Studies: Observational Research, Audits and Related Activities. New Zealand; 2006. Date accessed 15/05/2005. www.neac.health.govt.nz/moh.nsf/pagescm//520/$File/ethicalguidelines.pdf

(63) National Health and Medical Research Council, Australian Research Council, Australian Vice-Chancellor's Committee. National Statement on Ethical Conduct in Human Research. Government of Australia; 2007.

(64) The Bioethics Advisory Committee. Personal Information in Biomedical Research. 2007. Date accessed 15/06/2010. www.bioethics-singapore.org/uploadfile/15654%20PMPI%20Report.pdf

(65) World Health Organization (WHO). Handbook for Good Clinical Research Practice (GCP): Guidance for Implementation. Geneva; 2002. Date accessed 20/05/2006. http://whqlibdoc.who.int/publications/2005/924159392X_eng.pdf

(66) World Health Organization Regional Office for the Eastern Mediterranean. A Practical Guide For Health Researchers - WHO Regional Publications Eastern Mediterranean Series 30. Cairo; 2004. Date accessed 20/06/2010. www.emro.who.int/publications/pdf/healthresearchers_guide.pdf

(67) Saxena N, MacKinnon M.P, Watling J, Willison D, Swinton M. Understand Canadian's Attitudes and Expectations: Canadians' Dialogue on Privacy and the Use of Personal Information for Health Research in Canada. Canadian Policy Research Networks: Public Involvement Network; 2006. Report No.: Pl09.

(68) Ohm P. **Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization**. *Social Sciences Research Network (SSRN)*; 2009.

(69) The Academy of Medical Sciences. Personal Data for Public Good: Using Health Information in Medical Research. A Report from the Academy of Medical Sciences. London; 2006.

(70) Tu V.J, Willison DJ, Silver FL, Fang J, Richards JA, Laupacis A, et al. **Impracticability of informed consent in the registry of the Canadian Stroke Network**. *New England Journal of Medicine* 2004;**350**(14):1414-21. www.NEJM.org

(71) Government of Canada. Government of Canada Security Policy; Protected Information Fact Sheet. 2005.

**Title**

What are Canadian university biomedical research ethics boards (REBs) requirements for protecting privacy? A descriptive review of REB website-sourced policy and research protocol requirements.

**Author**

Mary Lysyk
University of Ottawa
Institute of Population Health
1 Stewart St. Room 300
Ottawa, Ontario, Canada
K1N 6N5

**Author's Contribution**

I, the doctoral candidate (ML), assumed responsibility for this research project. I was responsible for the conceptualization of the project, and led and conducted the different phases of the work including data collection, data analysis, overall synthesis and preparation of the manuscript.

**Acknowledgements**

I am grateful for the supervision of Dr. Ian Graham (Associate Professor, School of Nursing) who provided comments on the concept of the project and carefully reviewed the different drafts of this manuscript. Elyse Gagné, University of Ottawa, provided copy editing for the completed manuscript.

Patrick Moreau (PM), Research Assistant, Access to Information and Privacy Policy Department, Health Canada, provided independent random review of three REB website documents in the current revised manuscript. As well, PM verified the items of the CIHR BPPP list. John Horovath, (JH), CIHR Privacy Advisory Committee member & Senior Policy Advisor, Access to Information and Privacy Policy Department, Health Canada also independently verified the items of the CIHR BPPP list.

**Funding**

In-kind funding support was provided by the Access to Information and Privacy Policy Department, Health Canada.

# CHAPTER 5:
# WHAT ARE CANADIAN UNIVERSITY BIOMEDICAL RESEARCH ETHICS BOARDS (REBs) REQUIREMENTS FOR PROTECTING PRIVACY? A DESCRIPTIVE REVIEW OF REB WEBSITE-SOURCED POLICY AND RESEARCH PROTOCOL REQUIREMENTS


## Abstract

**Background**: Little is known about how Canadian research ethics boards (REBs) assess and manage privacy, confidentiality and security risks when reviewing research protocols. The few studies that have been conducted have shown widely varying and inconsistent practices across REBs. None have examined the degree to which the Tri-council Policy Statement Ethical Conduct for Research Involving Humans (TCPS 2) and the CIHR Best Practices for Protecting Privacy in Health Research (BPPP) are applied in REB website-sourced, i.e., publicly available from the REB website, policy and research protocol requirements. Given the Canadian public's concerns regarding the personal health information (PHI) privacy, and with the pervasiveness of advancing technologies, understanding how privacy is protected in the health research context is particularly timely.

**Objectives:** The overall objective of this descriptive study is to assess the privacy protection requirements of Canadian university biomedical REBs and to identify "new" or "innovative" REB privacy practices to protect PHI.

**Methods**: All 17 Canadian Faculty of Medicine (FoM) university based biomedical REBs were considered for inclusion in the study. REB policy and website-sourced research protocol requirements were the focus of the study. The TCPS 2 and CIHR BPPP guidance documents were converted to list form in order to allow for systematic comparison with REB documents. An additional coder verified 15 % of document analysis.

**Findings**: REB documents were available for 14 of 17 of FoM REB's. Key findings include: 1) there is broad consistency in terms of core privacy principles utilized across the REBs studied; 2) secondary use scenarios show the highest uniformity (mean 70%) in term of inclusion of items from the combined "master list" from both TCPS 2 and CIHR BPPP; 3) REBs are attempting to provide guidance particularly in terms of the development of prospective general-use databases; 4) the heterogeneity of practice detail across FoM REB website policy and application documents is high; and 5) while both the TCPS 2 and CIHR BPPP advocate a proportional approach to privacy risk management, they do not provide methods for REBs, and REBs studied are thus able to offer researchers little with which to accomplish this.

**Discussion:** This study represents the first time that Canadian REB website-sourced documents have been examined and compared to understand how they recommend that privacy is protected. Overall, REB FoM policy documents are generally adherent to core privacy principles. Where there are gaps, REBs use additional practices not present in either the TCPS 2 or CIHR BPPP. However, the health research community may need more guidance in order to make the job of good governance and privacy protection easier and less ambiguous for both researchers and REBs, particularly in the areas of secondary uses of data, creation of prospective databases and applying a proportional approach to privacy risk management. Additional guidance would also be valuable in building public trust that PHI is protected with advancing technologies.

## Background

Throughout most of the Western industrialized world, the responsibility to ensure the protection of privacy in health research studies takes place as part of research ethics reviews conducted by institutional research boards: (IRBs-United States); research ethics committees (RECs-Europe); human research ethics committees (HREC-Australia, New Zealand); and research ethics boards (REBs-Canada) [1-3]. National and international guidelines define the nature and scope of responsibilities for these ethical review committees [1-3].

When reviewing health research protocols in Canada, REBs apply relevant laws, ethics and privacy protection guidelines to study submissions [3]. REBs make available on their websites detailed guidance documents outlining protocol requirements for review of research studies. Protocol submission review is only one stage of a full board review; REB discussion/deliberation and, in some cases, a meeting with the principle investigator follows. Regardless, research protocol submission based on the available website policy and protocol requirements serves as the primary focus of the review and as such, should be as comprehensive as possible in order to facilitate a successful application.

Few studies have empirically examined how Canadian REBs assess and manage privacy, confidentiality and security risks when reviewing research protocols [4-6]. The studies that have been conducted are qualitative in nature and specifically look at REB decision-making about different case scenarios related to waiver of consent, the secondary uses of data, as well as the development of registries [4-6]. Findings from those studies show widely varying privacy practices across REBs, particularly regarding consent requirements in secondary use scenarios and in the development of clinical registries [4-6]. These findings also reveal REBs' relatively rudimentary understanding regarding some privacy issues, e.g., the application of safeguards, as well as REB concerns over reconciling domestic laws with the requirements of the Tri-Council Policy Statement and laws in other jurisdictions [5;6]. These studies also highlight that REBs generally welcome guidance and better education not only for themselves, but also for researchers and for patients [5;6]. One of the studies recommends that written REB policies and documentation should be examined in order to

see if the qualitative findings can be corroborated through a review of research protocol requirements [6].

This study will focus primarily on examining website-sourced, i.e., publically available from the REB website, policy and research protocol application requirements for research proposals undergoing full board review by Canadian university biomedical faculty of medicine REBs. It will highlight three areas in particular related to electronic health information and will include: the waiver of consent requirements for secondary uses of personal health information (PHI); development of general-use databases; and the application of a proportional (scaling protections to appraised privacy risks) approach to privacy protection [4-7].

Any study of REBs should first acknowledge that REBs are not accredited in Canada (and therefore are not subject to audit or process review) nor have current REB processes ever been formally examined to determine effectiveness at protecting the public [6-9]. As REBs represent a principle governance authority for ethical research in Canada, empirical study will add greatly to understanding not just privacy protection in health research, but also REB processes and procedures in the broader sense.

**Research objectives**

1) To assess the website-sourced privacy protection requirements of Canadian university biomedical faculty of medicine (FoM) REBs against both Tri-council Policy and guidance (elective) privacy, confidentiality and security practices available in Canada.
2) To assess the website-sourced privacy protection practices of FoM REBs in three areas that are particularly relevant to advancing technologies: waiver of consent requirement for the secondary uses of data, creation of prospective databases for general use, and the use of a proportional approach to managing risks to privacy, confidentiality and security.

3) To identify additional privacy practices regarding the protection of privacy, confidentiality, and security of PHI as required by FoM REB website research protocols.

**Conceptual framework**

The Trust-Risk Privacy Theoretical Framework was used as the conceptual framework for this manuscript study [10-12]. It is comprised of 6 privacy dimensions which are consistent with Fair Information Principles (FIPs) [10-12]. As FIPs form the foundation principles for privacy legislation not only in Canada but internationally, the fact that Framework elements are congruent with FIPs shows that they are appropriate for mitigating privacy risk [10;12]. The Framework has been validated by examining the use of personal information in e-commerce settings [10;12]. The six dimensions include: *control* over personal information; *collection* of personal information; *transparency/awareness* of privacy rights and organizational privacy practices; *preventing unauthorized access*; *authorization for health research* (secondary uses); and the influence of these dimensions on trust and risk-beliefs in terms of ultimately releasing personal health information [10;12].

It is the element on authorization for health research that is of primary interest in this study. In the Framework, authorization for health research is concerned with obtaining adequate consent and/or authorization for research (secondary uses) as well as utilizing safeguards as a way of mitigating risk of privacy breach while enhancing public trust [10;12]. With single discrete studies expanding into prospective disease or treatment-based databases without clear research questions, and the expected large scale demand of secondary uses of PHI from electronic health record systems (EHRs), advances in technology offer much promise for facilitating health research endeavors [6;13-15]. However, the increased risks to privacy need to be managed [6;13-15]. The Framework indicates that if privacy is not adequately protected, and the public perceives that risks of releasing PHI for health research purposes is too great, trust with the health research process will be reduced and the public will be less likely to participate [10;12]. Conversely, the Framework states that increased trust resulting

from adequate consent and/or from authorization for health research (both primary and secondary uses), as well as utilizing safeguards, will result in enhanced public trust and an increased likelihood the public will provide their PHI for research initiates [6;13-15].

The Framework does not provide specific privacy practices for researchers and REBs to follow. The privacy protection items combined from the TCPS 2 policy document and the CIHR BPPP guidance document provide detailed privacy protection practices both required and suggested.

## Methods

### *University Faculty of Medicine REB privacy practices*

All FoM REBs in Canadian universities are the focus of this study. They were selected due to the varied and complex nature of the protocols that are reviewed by these REBs, and in many cases, organizations such as hospitals and other primary care facilities utilize these REBs to provide research ethics review for them. This means that FoM REBs are likely subject to the full spectrum of biomedical research protocols and thus face a wide range of privacy protection issues.

### *Inclusion/exclusion of FoM REBs*

All university FoM biomedical REBs in Canada were initially sought for inclusion. The sampling frame began with a list of 17 university faculties of medicine in Canada obtained from the Association of Faculties of Medicine of Canada (AFMC) website [16].

REBs were excluded if: a dedicated biomedical REB did not exist for that FoM; REB policy documents were not publically available; and if REB application forms, templates and processes were not publically available. For example, if access to REB documents required a unique university identifier number and password, that REB was excluded.

***Inclusion/exclusion criteria for selection of FoM REB website research protocol documents***

For each university FoM biomedical REB, websites and links were carefully examined. All documents related to protocol submission privacy requirements including policy and guidelines such as application forms, templates, e.g., assent and consent templates, and accompanying supporting documents for full board review, as well as any specific reviews for secondary uses and database research, were printed and compiled for comparative analysis. Documents written in English or French were accepted.

As the focus was on general full board review, documents or contents were excluded if: they related to specific types of research or populations (children and youth, aboriginal communities) or involved complex or unique privacy protection regimes (human biological materials, genetic or genomic research or clinical registries).

The review was first conducted in October 2010 and updated April 4-7, 2013.

***Comparison with Canadian privacy protection policy and guidance documents***

In order to have a systematic method of comparison, the privacy practices identified in Canadian policy and guidance documents, specifically the TCPS 2 and CIHR BPPP were combined and itemized. As the CIHR BPPP contains the most practices (158), it was itemized first. The content of the CIHR BPPP lists were then verified by a research assistant (PM) and, a member of the CIHR Privacy Advisory Committee (JH) (**Appendix 1**). The TCPS 2 document was then compared to this list of validated CIHR BPPP items (Appendix 2). One hundred and two similar practices were identified along with four additional ones not included in the CIHR BPPP, for a total of 106 items. The four additional practices, which included two related to obtaining ongoing consent from participants and two identifying secondary use scenarios excluded from REB review, were added to the 158 items of the CIHR BPPPs list to create a combined listing of 162 privacy practices (**Appendix 1**).

***Total list of all items (TCPS 2 and CIHR BPPP)***

The total or "combined" or "master" list of practices grouped according to the 10 CSA Model Code of fair information privacy principles (as adapted by CIHR for health research) [17], provided a systematic method to examine the university biomedical REB website research protocol requirements. The principles include: 1) Determining research objectives; 2) Limiting collecting of personal information data; 3) Consent requirements; 4) Managing consent; 5) Informing prospective participants about the research through informed consent; 6) Recruiting participants; 7) Safeguarding personal data; 8) Controlling access; 9) Retaining data; and 10) Accountability and transparence [17]. The policy and guidance documents were combined into one list as the goal of the study was to identify what privacy protection measures were identified for research protocol review and what additional ones exist. Use of the "master list" is intended to allow comparison not as an indicator of REB application or policy document quality, i.e., more items does not imply a "better" document. Nor does it suggest a "list of things to be checked off" by researchers or research ethics review boards.

Data management for the item-by-item comparison between the list of 162 privacy practices and the REB website-sourced research protocol requirement documents was done using the Microsoft Excel program.

For ease of analysis, the 162 items from the list were also grouped according to the CIHR adapted CSA Model Code 10 privacy principles described above [17].

All of the REB website research protocol documents were extracted and reviewed by one reviewer (ML). An additional reviewer (PM) replicated the reviews on a random sample of 3 REB website documents. Comparison was 95% for the use of master list of 162 privacy practices and 90% for identification of additional items. The primary reviewer typically identified more items from both scenarios.

Website protocol requirements were next examined to determine the degree to which they incorporated TCPS 2 privacy practices.

Using the Excel program, the website-sourced REB documents were examined item-by-item to identify other provisions for protecting privacy in the health research not appearing in the "master list" of practices.

## Findings

Of the 17 possible university biomedical faculty of medicine REBs, three were excluded. Two due to password requirements for access to website documents while the other was excluded as the university facility did not have a dedicated REB and relied instead on other institutional REBs. Fourteen of 17 REBs (83%) remained for the analysis.

### *Objective 1: Privacy protection practices of Canadian university biomedical faculty of medicine REB in website research policy and protocol requirements in comparison with TCPS 2and CIHR BPPP.*

All of the REB website requirements stated that their protocol requirements were compliant with the TCPS 2. Ten of 14 (71%) required a sign-off by the principle investigator that the researcher has been compliant with the TCPS 2 in their protocol submission. None of the REBs required compliance with the CIHR BPPP, but 4 of 14 (29%) either recommend its use or provided a link to the document.

**Table 5-1** provides a summary of the comparative review of the university biomedical REB website research protocol requirements starting with whether they consider the 10 core privacy principles themselves in their REB application process. This was ascertained with the inclusion of at least one privacy practice/item related to that principle. Results show that with the exception of one principle by one REB (*Principle 10: Accountability/Transparency*; REB 14), all of the core principles were addressed in some way by the website research protocol requirements.

In terms of inclusion of specific practices, there is variation in the amount of privacy specific detail in protocol requirements available on REB website. Overall inclusion of the 162 specific privacy practices range from 25%-80% of items. A closer examination shows that

certain principles have a much higher inclusion of items (and thus more uniformity) than others. Those with the highest practice item inclusion and least variability include *Principle 6: Recruitment* (mean 58% of items), *Principle 1: Research objectives* (mean 58%) and *Principle 2: Limiting collection* (mean 56%).

The principles with the least detail (and most variability) in terms of inclusion of practice items were *Principle 7: Safeguarding personal data* (mean 32% inclusion of items), and *Principle 10: Ensuring accountability and transparency in the management of personal data* (mean 27% inclusion of items).

How the REB website documents incorporate the TCPS 2 practices is presented in **Table 5-3**. Compared to the combined items in **Table 5-1**, results are more uniform. Overall inclusion of TCPS 2 items range from 38%-97% (compared with 25%-77% of combined items). A review of each of the 10 privacy principle shows a much higher inclusion of items (40%-74%) in comparison with the combined list which shows a lower range of inclusion of items per principle (30%-59%). *Principle 7: Safeguarding personal data* (mean 55% inclusion of items), and *Principle 10: Ensuring accountability and transparency in the management of personal data* (mean 40% inclusion of items) continue to show the least detail.

***Objective 2: Overview of practices related to the secondary uses of data, creation of prospective data bases for general use, and the use of a "risk assessment and proportional management" strategy to protecting privacy.***

**Table 5-2** proved a summary of how the REB website documents addresses privacy practices related to the secondary uses of PHI, the creation of general use databases, as well as use of a "privacy risk assessment and proportional management" approach.

Twelve items from the "master list" of 162 items (**Appendix 1**) classified as specific to secondary uses can be broken down as follows: items related to request for waiver of consent considerations (six items), jurisdictional considerations (one item), possible community or group consultation (one item), and strategy for informing the public (one item). The

remaining three of the 12 items include that consent will be sought (one item) as well as two additional TCPS 2 secondary use items guiding when REB review is not required. Findings show that all REBs address secondary use to a relatively high degree and also include their specific jurisdictional requirements. All highlight conditions under which research may be exempt from requiring consent.

For general-use databases, the bulk of the 15 items from the "master list" (**Appendix 1**) were derived from CIHR BPPP. Six items related to the parameters of creating a database (defining scope, types of studies that can be undertaken, what the database will not be used for collection and types of data that are necessary). The remaining nine items specify what is to be included in the consent process, as well as data retention. A majority of REBs, 11 of 14 (79%), provide some type of guidance practices for general use databases, although low uniformity exists on this topic. The most common items relate to the documented consent process and include: identifying the types of studies that might be conducted (seven of 14 REBs; 50%); identifying any possible data linkages (seven of 14 REBs); identifying other data uses including expected commercial usages (six of 14 REBs); as well as authorization by the individual for future uses of data (four of 14 REBs).

Three of 14 REBs (21%) state the need for a "privacy risk management" approach to information/PHI protection. Details on how to accomplish this was largely left to the researcher.

**Table 5-1: Analysis summary by 10 privacy principles – faculty of medicine biomedical REBs (n=14)**
***Percentage of combined TCPS 2 and CIHR BPPP 162 list items identified in website sourced REB research protocol requirements**

| REB (n=14) | 1: Research objectives (including broad use databases) 12 items | 2: Limiting collection of personal data 12 items | 3: Consent requirement (including secondary use) 17 items | 4: Managing consent 8 items | 5: Informing participants 45 items | 6: Recruitment 13 items | 7: Safeguard 28 items | 8: Control access & disclosure 9 items | 9: Data retention 8 items | 10: Accountability transparency 10 items | *Total combined TCPS 2 + CIHR BPPP items 162 items |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Range of item inclusion | 4-12 items | 4-8 items | 4-15 items | 3-8 items | 14-37 items | 3-12 items | 4-24 items | 1-6 items | 1-6 items | 0-7 items | 41/162-130/162 (25%-80%) |
| Mean % | 6.7/12 (56%) | 6.7/12 (56%) | 8.6/17 (41%) | 4.5/8 (50%) | 24.2/45 (54%) | 7.6/13 (58%) | 8.9/28 (32%) | 3.7/9 (41%) | 3.6/8 (45%) | 2.7/10 (27%) | 77.3/162 (48%) |

**Table 5-2 Analysis summary of secondary use, prospective general-use database and use of privacy risk assessment and proportional management approach to protecting personal information (includes TCPS 2 and CIHR BPPP items)**

| | REB (n=14) Range | TOTAL *mean |
|---|---|---|
| 11.Second use (12 items) | 3-12 items | 8.4/12 (70%) |
| 12.General-use database (15 items) | 0-18 items | 5/15 (33%) |
| 13.Privacy risk assessment and proportional management approach (1 item) | 0-1 items | 0.2/1 (21%) |

***The percentage represents the number of PI protection list items that were included in the website sourced REB research protocol requirements**

**Table 5-3: Analysis summary by 10 privacy principles – faculty of medicine biomedical REBs (n=14)**
*** *Percentage of TCPS 2 106 list items identified in website sourced REB research protocol requirements**

| REBs (n=14) | 1: Research objectives (including broad use databases) 7 items | 2: Limiting collection of personal data 10 items | 3: Consent requirement (including secondary use) 13 items | 4: Managing consent 7 items | 5: Informing participants 32 items | 6: Recruitment 8 items | 7: Safeguard 14 items | 8: Control access & disclosure 4 items | 9: Data retention 4 items | 10: Accountability transparency 7 items | *Total combined TCPS 2 items 106 items |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Range** of item inclusion | 3-7 items | 3-10 items | 3-12 items | 3-7 items | 13-32 items | 2-8 items | 4-13 items | 1-4 items | 1-4 items | 1-3 items | 40/106-103/106 (38%-103%) |
| **Mean %** | 5.2/7 (74%) | 6.6/10 (65%) | 8.1/13 (62%) | 5/7 (71%) | 22.5/32 (70%) | 5.6/8 (71%) | 7.7/14 (55%) | 2.6/4 (64%) | 2.2/4 (57%) | 2.7/7 (40%) | 70/106 (66%) |

**Table 5-4: Analysis by 10 privacy principles: additional or variation protection of PI requirements (n=11 REBs)**

| | 1: Research objectives | 2: Limiting collection | 3: Consent (required or not) | 4: Managing consent | 5: Informing participants | 6: Recruitment | 7: Safeguard | 8: Control access & disclosure | 9: Data retention | 10: Accountability transparency |
|---|---|---|---|---|---|---|---|---|---|---|
| **REB 1** | | 4 | 1 | | | | 3 | 2 | | 1 |
| **REB 2** | | | | | 2 | | 3 | 3 | | 2 |
| **REB 3** | | 4 | | | 1 | | 3 | 1 | 1 | 1 |
| **REB 4** | | 1 | | | | | 2 | 1 | | |
| **REB 5** | | | | | 1 | | | 1 | 1 | |
| **REB 6** | | 2 | | | | | | | | 2 |
| **REB 7** | | | 1 | | | | 2 | 2 | | |
| **REB 8** | | 2 | | | | | 2 | 1 | | |
| **REB 9** | | | | | | | | 3 | | |
| **REB 10** | | | 1 | | 1 | | 2 | 2 | | |
| **REB 12** | | | | | | | | 1 | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| **Total (63)** | **0** | **13** | **3** | **0** | **5** | **0** | **17** | **17** | **2** | **6** |

***Objective 3: Other REB privacy practices regarding the protection of privacy, confidentiality and security of PHI as required by university biomedical REB website research protocols.***

Sixty-three (63) additional practices were identified from 11 of the 14 REBs studied (**Table 5-4**). None of the practices are interpreted as being in conflict or disagreement with the TCPS 2. While five could be considered as "innovative" or actual "tools". The remaining 58 are variations or provide further specification to those found in TCPS 2.

The 63 additional practices are classified under one of the 10 core privacy principles. Specifically, the largest number of additional new practices, 17, appears for both *Principle 7: Safeguarding personal data* and *Principle 8: Controlling access and disclosure*. *Principle 2: Limiting collection of personal data* has the second most, with 13 items (**Table 5-4**).

*Principle 7: Safeguarding personal data* expands on the combined list of items, but with a higher degree of specificity. For example, the need for clearly outlining breach protocol procedures includes the clauses that research subjects and the REB must be informed of the breach and must demonstrate that the research team has received privacy specific training. For databases, use of a Privacy Impact Assessment based on the CIHR BPPP is identified. For secondary uses, two of the REBs require researchers to complete the same web-based "Chart Review Tutorial" before they collect use or disclose PHI. *Principle 8: Controlling access and disclosure* includes items that require identification by name and justification for any individual that will have access to the data, and identification of an administrator who will be responsible for overseeing access controls, and creation and maintenance of a data access user log. An Internet research guidance document was also developed that provides strategies for controlling unauthorized access and disclosure for Internet-based studies. Finally, a Directive on Protection of Personal Information from Access Outside Canada is also in use. *Principle 2: Limiting collection of personal data* provides further limitations on direct identifiers that can be collected; that is, if a Personal Health Information Number is being collected, collection must be justified and a link to an online tool for data de-identification is provided (this last tool is also useful for disclosure situations in *Principle 8*.

## Table 5-5: Detailed Listing of Additional, Variation or Innovative Privacy Practices (n=63)

**University faculty of medicine biomedical REBs (n=11)**

| | |
|---|---|
| 1 | Identify requirements for data to be deemed de-identified |
| 2 | Use of Privacy Impact Assessment for large scale or collection of sensitive informatics |
| 3 | When using tissue or data from data banks describe process for obtaining consent from custodian of bank/registry; if tissue/data is not anonymized provide evidence that consent was obtained at time of collection |
| 4 | Acknowledge that responsibility for security of data rests with the primary investigator |
| 5 | Outline data safeguarding procedures when sending data outside the institution |
| 6 | Specify the names and affiliations of persons outside of your study team who will have access to the data |
| 7 | To individuals: what information will be retained in the event of their withdrawal from the study |
| 8 | Consent**:** subjects should receive notice of potential risks related to breach of privacy |
| 9 | Outline procedure to respond to breaches of confidentiality (must inform both subjects and REB) |
| 10 | Explain how security and confidentiality of data will be maintained when research records are archived off-site |
| 11 | Provide list of personal identifiers to be included in disclosures of research data |
| 12 | Indicate the entity or person who will retain custody of the data and the address of the database |
| 13 | All PHI that leaves the site must be de-identified, password protected, and encrypted |
| 14 | Outline safeguarding procedures when sending data outside the institution |
| 15 | Specify the names of persons outside of your study team who will have access to the data |
| 16 | Specify who has access to listing of names and study ID #s |
| 17 | Are alternatives to participating in research clearly explained? |
| 18 | Identify all sources of data to be accessed |
| 19 | Outline data safeguarding procedures at institutions receiving data |
| 20 | Specify the names and affiliations of persons outside of your study team who will have access to the data |
| 21 | List all external servers and portable devices on which micro data may be stored |
| 22 | Will you be receiving data from external sites? |
| 23 | For secondary use**:** Are any sensitive issues raised in the study that may require subject consent, i.e. HIV status, mental health issues? If yes, justify not getting patient consent and outline additional safeguards |
| 24 | For transborder flow of data**:** indicate how security and consent implications for international implications, i.e. US Homeland Security, have been addressed in the Directive on Protection of Personal Information from Access Outside Canada |
| 25 | Outline procedures for responding to a breach of confidentiality (include individual whom principal investigator should contact in case of breach) |
| 26 | Research team has received privacy-specific training – Chart Review Tutorial |

| | |
|---|---|
| 27 | Identify potential privacy, confidentiality, psychological, emotional, social, and economic risks |
| 28 | For anonymized data: Identify any third-parties who will have access to study data |
| 29 | Outline retention and disposal procedures for nominative/coded data and anonymous data |
| 30 | Identify administrator responsible for overseeing access controls |
| 31 | Consent: Outline withdrawal procedures; include retention and disposal procedures for data from subjects who withdraw |
| 32 | Describe physical security procedures, i.e. identifiers removed from paper records, all research team members have signed an oath of confidentiality, paper and electronic records are secured. |
| 33 | List identifiers to be retained and provide give rationale for retention |
| 34 | Identify all sources of data that will be accessed |
| 35 | Outline data safeguarding procedures when sending data outside the institution |
| 36 | Identify all agencies or individuals other than the research team who, for monitoring or auditing purposes, may require access to identifiable or confidential data collected for this research |
| 37 | Demonstrate compliance with all relevant legislation |
| 38 | Acknowledge that PHI will not be published in identifiable form, and that PHI will be used exclusively for the purpose of the approved research project |
| 39 | Legislative compliance not required when identifiable information is replaced with a unique code |
| 40 | Describe process for the creation and maintenance of a user log for a database containing identifiable PHI |
| 41 | Specify the names and affiliations of persons outside of your study team who will access to the data |
| 42 | List all external servers and portable devices on which micro data may be stored |
| 43 | Specify potential privacy risks, i.e., potential to associate specific information in data with a specific participant, possibility that third parties will be exposed to loss of confidentiality, social risk, potential loss of status/reputation. |
| 44 | Indicate how data will be used (i.e. thesis, journal article, conferences) |
| 45 | Identify the person who will be responsible for data storage |
| 46 | Indicate who will supervise who has access to the data |
| 47 | Describe procedures used to obtain research data |
| 48 | Identify all sources of data that will be accessed |
| 49 | List personal identifiers to be retained after completion of data collection and justify each |
| 50 | Outline data safeguarding procedures when sending data outside the institution |
| 51 | Identify all agencies or individuals other than the research team who, for monitoring or auditing purposes, may require access to identifiable or confidential data collected for this research |
| 52 | For secondary use: Justify (statistically) the collection of minimal number of records required to address research question/hypothesis |
| 53 | Outline organizational protocols for and procedures for responding to breach of privacy/confidentiality |
| 54 | Research team has received privacy-specific training |
| 55 | Identify privacy, confidentiality, psychological, emotional, social, and economic risks and stressors |
| 56 | Has hospital Privacy Officer or ethics office been consulted regarding privacy and security issues? |
| 57 | Does the study involve deception or intentional lack of disclosure? |

| | |
|---|---|
| 58 | Consent: participants are informed that REB may contact them or require access to study-records to monitor conduct of research |
| 59 | Internet research guidelines provided |
| 60 | Demonstrate compliance with relevant privacy legislation in all stages of research |
| 61 | Specify if a survey company will be used in data collection, storage, or analysis |
| 62 | Outline data safeguarding procedures when sending data outside the institution |
| 63 | Use of web based tool to identify risks of data re-identification |

## Discussion

### *Chief findings*

This study reveals five key findings. The first is that, at a high level, there is broad consistency in terms of website-sourced FoM REB policies and practices across REBs. For example, all of the REBs studied indicated compliance with the TCPS 2 policy document. With only one exception, FoM REBs studied were found to address all of the 10 core privacy principles in some way. In further support of this point, the vast majority of additional practices, 92% (58 of 63), are simply variations or provide further specification to those found in TCPS 2.

It is reassuring that compliance with TCPS 2 appears relatively high (overall mean inclusion of items is 66%: **Table 5-3**) in the sample studied, given that the TCPS 2 is the most influential Canadian policy applicable to the ethics of research with human participants and widely followed by Canadian researchers and institutions. It is also clear where there are gaps in the actual REB research protocol requirements, researchers are typically expected by the REBs to turn to the TCPS 2 first for direction.

The second main finding of the study is that secondary use scenarios show the highest uniformity (mean 70%) in terms of inclusion of items from the combined "master list" from both TCPS 2 and CIHR BPPP. However, despite this high uniformity, the qualitative study that examined waiver of consent practices found a high degree of variability in decision making practices by university faculty of medicine REBs [6]. The authors felt that this may reflect ambiguity on the part of TCPS [6]. Even though the TCPS has been updated since the Willison et al study was published in 2008, the secondary use article of the TCPS 2 has

changed very little in terms of additional detail (two items have been added regarding waiver for publically available or anonymized data). In this 2008 study, REBs did request more detail in the TCPS and review templates for research involving the secondary use of data. In order to provide further detail and guidance regarding the secondary uses of PHI, CIHR sponsored the development of secondary use "best practices" which became available in 2006 [18]. It was available (in hardcopy and CD) at a nominal cost to the research community and included a toolkit of checklists and considerations [18]. When the current study examined reference documents that the sample REBs are using, the "secondary use best practices" were not listed by any of the REBs. Understanding why this guidance document is not more widely used given that the concepts presented in it are still highly relevant, would provide valuable information in understanding overall REB and researcher needs in terms of secondary use scenarios.

The third finding relates to the creation of prospective general-use databases. The TCPS 2 offers very little guidance that is specific to this activity and none related to activities such as the development of registries. In fact, few changes exist between the first and current versions of the TCPS 2. The REBs studied, however, attempt to provide detail in this area on their websites policies and application forms. This finding is consistent with previous work that examined the decision making process of REBs specifically related to the development of registries and once again shows that further detail and guidance is needed [4].

The fourth substantive finding relates to the relatively high heterogeneity of detail present across FoM REB website-sourced policy and application documents. The amount of detail ranges from 41%-74% (mean inclusion) of TCPS 2 & CIHR BPPP combined practice items. However, the variation is understandably much lower when compared to TCPS 2 policy provisions on their own (38%-97%). Nevertheless, significant variation does exist. Without contacting the REBs themselves, it is difficult to know the reasons for this large range.

The variation may relate to the types of protocols that are reviewed at the institution and the use of broader questions in the application process. With the use of broader questions, the

onus largely on the researcher to provide details. For example, instructions such as: "Describe how data will be protected" and "Describe confidentiality and how it will be maintained", were common. While it is it clear what impact (if any) this has on research protocols, less detail does allow more latitude for researchers regarding the exact practices that are needed. However, it is also possible that less detail can result in uneven protection of research subjects [5; 6].

The area with the lowest inclusion of research protocol privacy detail relates to practices that include the designation of an individual to be accountable for privacy within a research initiative. Another area of low inclusion is the transparency of relevant privacy policy for study participants. Omission of these items can lead to participants not knowing their privacy rights or whom to contact in case of privacy questions or concerns [19]. For the research team, lack of accountability can affect team members' adherence to privacy polices[19].

Safeguard requirements for protecting data is an area that shows a lower inclusion of items. In addition, it shows a variation both in terms of inclusion of the combined items as well as TCPS 2 requirements. This finding confirms previous studies that have examined this area [20]. Interestingly, safeguarding data is also one of the areas with the largest number of innovative practices by FoM REBs. This suggests that, with the threats to privacy posed by advancing technologies, REBs may be struggling to understand which safeguards to recommend regarding data security. In support of this position, the few high-profile privacy breaches in health research reported in the media over the last few years point to inadequate safeguards as the primary cause. For example, in December 2010, the national media reported that a laptop belonging to a researcher at the University of Alberta that contained the medical information of 2,700 research subjects was stolen [25;26]. According to the Alberta Information and Privacy Commissioner, the paramount concern was that the data was not adequately encrypted or protected [25;26]. Around the same time, and again in Alberta, a laptop went missing that belonged to a genetic research company that included highly sensitive personal information such as social insurance numbers [25;26]. Once again, a lack of encryptions and privacy protection measures was concluded to be the problem [25;26]. In

2007, a laptop containing the medical information of 3,000 patients enrolled in research study at the Hospital for Sick Children was stolen from the researcher's unattended vehicle in a shopping mall parking lot [21]. Once again, none of the data had been properly encrypted or protected [21].

The last finding very simply observes that, while both the TCPS 2 and CIHR BPPP advocate a proportional approach to privacy risk management, they do not provide insight to how REBs and researchers should go about doing this, and as a result, REBs studied were thus not able to provide researchers with much detail. This is clearly an area that further direction and guidance would be valuable for the health research community.

The Trust-Risk Privacy Theoretical Framework indicates that awareness of privacy breaches by the public will decrease trust that PHI is protected in the research context and will decrease the likelihood that the public will provide their PHI in research contexts. Preventing breaches with appropriate security measures is therefore of paramount importance in maintaining public trust [22].

***Limitations of the research***

Without input from committee members of REBs studied as well as researchers, it is not known whether FoM biomedical REBs use more privacy considerations and criteria than just those documents available on their website when reviewing research protocols. Specifically, it may mean that additional REB review processes that could have offered more insight into the requirements of research protocols have been omitted. The findings likely represent the minimum requirements of REBs. However, as previous studies have utilized qualitative methodologies and have focused on the decision-making process with similar findings, this study serves to corroborate the previous results.

Other limitations include:

- Two website-sourced FoM REB documents could not be accessed due to password requirements, i.e., restricted access in the public domain. The two REBs could

potentially have privacy requirements that differ from those that are in the public domain. Generalizability to all university faculty of medicine REBs is therefore limited.

- Focusing on only one population of REBs greatly limits any generalizability of results. Including more categories of REBs and in particular those that deal with sensitive PHI, e.g., mental health institutions, hospital based REBs or REBs that review protocols primarily for vulnerable populations such as children and the elderly would provide significant insight into how these REBs protect PHI given the added risks to privacy involved. Including REBs from different contexts, e.g., private REBS, academic, and clinical based, would allow for a comparison of PHI protection provisions in different environments. Additionally, including human biological materials, review of genetic protocols and other highly complex topics will add significantly to the understanding of REBs' decision-making in these complex areas.

The Trust-Risk Privacy Theoretical Framework offers a paradigm for understanding how privacy protection measures can impact the public's trust and risk beliefs when providing PHI in the research context; however, it does not provide sufficient detail to explain which privacy protection items should be included and can have the most impact at minimizing privacy risks and maximizing trust. As well, its lack of specificity in the health research context also limits the overall guidance it can offer. One suggested method to address this issue is to use the "combined list" of items from the TCPS 2 and CIHR BPPP. Future studies utilizing the Framework in health research contexts would greatly add to the Framework's validity and overall usability for the health research community.

Furthermore, the TCPS 2 list of items did not benefit from verification by an independent party as did the CIHR BPPP item list. This increases the risk of possible misclassification of these items.

Finally, further research is needed in order to provide more in-depth analysis and interpretation, particularly in terms of the decision-making process REBs use when reviewing actual research protocols.

***Policy implications and directions for future research***

Findings from this study confirm previous qualitative work that shows variation in requirements across REBs by quantifying the variation in privacy practices. In the case of secondary use of data, REBs apply a high level of detail available in both the TCPS 2 and CIHR BPPP; however, this does not lead to more consistent decision-making regarding research protocols using this methodology [6]. Inconsistent practices by REBs may introduce uneven protection of human subjects and variability in research protocol requirements [6].

Canadian laws provide considerable scope for self-governance on the part of the research community [23]. Therefore the onus is on the research community to ensure that systems are in place that will engender public trust that their personal information is protected [23]. Both the TCPS 2 policy and CIHR BPPP guidance documents advocate a "privacy risk management" approach that essentially promotes an assessment and proportional method for managing privacy risk (however detail is not provided on how researchers should achieve this). To address this gap, the "master list" of PHI protected practices along with the new practices that emerge could be converted to an "online" decision tree that would guide researchers through the privacy risk assessment and mitigation process. The "combined list" could be used to develop standards to facilitate systematic approaches to implementing privacy practices, audit of information use practices/safeguards and to strengthen reporting relationships with the Information/Privacy Commissioner. These uses all represent key privacy oversight requirements for preserving public trust as outlined in the Trust-Risk Privacy Framework [23].

Since the international health research community is also able to offer little regarding the application of safeguards within the advocated "privacy risk assessment and management" approach [3;17;24]. Future areas of research could include identifying models from other sectors that could be used in the health research context as well as canvassing researchers and REBs regarding their specific needs in this area.

## Conclusion

Currently in Canada, REBs, which form the apex of health research governance, are not subject to audit and have been studied very little in terms of decision-making processes [6-9]. To the author's knowledge, this study represents the first time that website sourced research protocol requirements have been examined to see how they are ensuring that personal information is protected in health research protocols. Overall, FoM biomedical REBs studied appear adherent to core privacy principles as well as the TCPS 2. Where there are gaps, the REBs studied use additional practices not present in either the TCPS 2 or CIHR BPPP. Yet researchers and REBs may need more in order to make the job of good governance and privacy protection easier and less ambiguous, particularly in the areas of secondary uses of data, creation of prospective databases and applying a proportional approach to privacy risk management.

Since neither the TCPS 2, CIHR BPPP, nor similar international documents provide more guidance in these areas, identifying researcher and REB needs and turning to other sectors for strategies may prove useful in narrowing the gap that translates requirements into practices [3;17;24]. This is particularly the case for applying a proportional approach to privacy risk management in general to health research and in the application of safeguards specifically. The additional 63 privacy protection items may prove helpful in the development of standards that can be applied towards proportionality, harmonization and ultimately rigorous efforts to protect privacy [7;22;25].

## REFERENCES


(1) *The Data Protection Directive and Medical Research Across Europe*. Aldershot: Ashgate Publishing Limited; 2004.

(2) *Research Ethics Committees, Data Protection and Medical Research in European Countries*. Aldershot: Ashgate Publishing Limited; 2005.

(3) Tri-Council Policy Statement : Ethical Conduct of Research Involving Humans - Second Edition, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (2012).

(4) Gibson E, Brazi K, Coughlin MD, Emerson C, Fournier F, Schwartz L. **Who's minding the shop? The role of Canadian research ethics boards in the creation and uses of registries and biobanks.** *BioMed Central Medical Ethics* 2008;**9**(17):1-9. Date accessed 11/04/2011.www.biomedcentral.com/1472-6939/9/17

(5) Ouellet R. **Privacy issues and the Canadian Medical Association** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011. p. 93-110.

(6) Willison DJ, Emerson C, Szala-Meneok K, Gibson E, Weisbaum K, Fournier F. **Access to medical records for research purposes: Varying perceptions across Research Ethics Boards.** *Journal of Medical Ethics* 2008. Apr;**34**(4):308-14. doi: 10.1136/jme.2006.020032

(7) Willison D, Gibson E, McGrail K. **A Roadmap to Research Uses of Electronic Health Information.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011.

(8) Hebert P, Saginur R. **Research ethics review: Do it once and do it well.** *Canadian Medical Association Journal* 2009 Mar 17;**180**(6):597. Date accessed 08/11/2011. www.cmaj.ca/content/180/6/597.full.pdf+html

(9) Knoppers BM. **Challenges in ethics review in health research**. *Health Law Review* 2009;**17(**2-3):47-52. Date accessed 07/03/2013. http://www.hli.ualberta.ca/en/HealthLawJournals/~/media/hli/Publications/HLR/17-23-06_Knoppers.pdf

(10) Malhorta NK, Kim SS, Agarwal J. **Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model.** Information Systems Research 2004;15(4):336-55.

(11) Saxena N, MacKinnon M.P, Watling J, Willison D, Swinton M. Understand Canadian's Attitudes and Expectations: Canadians' Dialogue on Privacy and the Use of Personal

Information for Health Research in Canada. Canadian Policy Research Networks: Public Involvement Network; 2006. Report No.: Pl09.

(12) Smith HJ, Milberg SJ, Burke SJ. **Information privacy: Measuring individuals' concerns about organizational practices.** *MIS Quarterly* 1996;**20**(2):167-96. www.jstor.org

(13) Willison DJ. **Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward**. *Journal of Health Services Research and Policy* 2003;**8**(1):S1:17-S1:23.

(14) Willison DJ. **Trends in collection, use and disclosure of personal information in contemporary health research: Challenges for research governance.** *Health Law Review* 2005;13(2&3):107-13.

(15) Willison DJ, Schwartz L, Abelson J, Charles C, Swinton M, Northrup D. **Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public?** *J Am Med Inform Assoc* 2007;**14:**706-12. Doi 10.1197/jamia.M2457

(16) The Association of Faculties of Medicine of Canada/ L'Association des facultes de medecine du Canada. 13 A.D. Apr 4; 2013.

(17) Canadian Institutes of Health Research. CIHR Best Practices for Protecting Privacy in Health Research. Ottawa: Public Works and Government Services Canada; 2005. Date accessed 20/05/2006. www.cihr-irsc.gc.ca/e/29072.html

(18) Slaughter PM, Collins PK, Roos N, Weisbaum KM, Hirtle M, Williams JL. Privacy Best Practices for Secondary Data Use; Harmonizing Research & Privacy: Standards for a Collaborative Future. Privacy Best Practices for Secondary Data Use (SDU) [CD-ROM] (2006).

(19) Cavoukian APIaPCoO. 20/20 Access & Privacy Excellence... 20 Years in the Making. 20th Anniversary Collection. Toronto, Ontario: Information and Privacy Commissioner of Ontario; 2008.

(20) Borfitz D. Conspiring Forces Behind EDC Adoption. CenterWatch 10[2]. 2003. Ref Type: Magazine Article

(21) Brand R. **Overseas antidote: medical services are moving offshore, raising privacy issues.** *Rocky Mountain News* 2005 May 21.

(22) Lowrance WW. *Privacy, confidentiality and health research*. Cambridge: Cambridge University Press; 2012.

(23) Gostin LO, Turek-Brezina J, Powers M, Kozloff R. **Privacy and security of health information in the emerging health care system. Health Matrix**: *Journal of Law -*

*Medicine* 1995;**5**(1):1-36. Date accessed 12/12/2005. www.critpath.org/msphpa/ncshdov.htm

(24) Lysyk M. *A descriptive comparison of international and Canadian guidelines in health research privacy* .University of Ottawa. Ottawa, Ontario (2013).

(25) Chadwick R, Strange H. **Harmonization and standardization in ethics and governance: Conceptual and practical challenges.** In: Widdows H, Mullen C, editors. *The Governance of Genetic Information: Who Decides?* Cambridge: Cambridge University Press; 2009. p. 201-13.

# CHAPTER 6:
# INTEGRATION OF THESIS FINDINGS AND IMPLICATIONS

## Background

As a result of a revolution in information and communication technologies, health research activities are changing globally [1-4]. More specifically, information technology is changing health research in three major ways: 1) it allows new types of measurements (or new techniques) such as digital data from magnetic resonance images of the body, geospatial location information and information derived from—or contained within—DNA; 2) it makes collection, storage, transfer, analysis and retrieval of large amounts of data easy, fast, inexpensive (and the devices that store this data ultra-portable) and therefore ubiquitous; and 3) it allows for the globalization of health research by facilitating dissemination, sharing and linking of large amounts of information [5]. These advances have facilitated a change in the types of research being conducted [1-4]. For example, single, time-limited studies with clearly defined research questions are evolving into international programs of research that require prospective collections of large data sets containing PHI [2;4;6]. The intention is that these data sets will be used for numerous future studies for which the research questions are not yet known and without clear end dates as to how long the data sets will be maintained [2;4;6].

Another concrete example of the e-health revolution is the increase in use of electronic health records (EHRs) in patient care in many westernized countries such as the United States, Australia, New Zealand, Canada and the United Kingdom [6-8]. Secondary uses of PHI for health research accessed from EHRs can potentially offer a tremendous source of rich cradle-to-grave data [6-8]. The potential that general-use databases and the secondary uses of data (from multiples sources) hold for understanding and recognizing the many factors that influence the health status of individuals and populations is well recognized [7-9]. However, these new opportunities present many privacy challenges and touch on the interests of many stakeholders in the health research community. Some of the key issues raised by stakeholders are summarized as follows [7;10] :

**Health researchers** are concerned that privacy laws, along with multiple rules, policies and procedures, present impediments to their ability to conduct beneficial research when using both primary and secondary data sources [4;7;8]. As it is, researchers are currently required to fulfill numerous administrative requirements from their academic institutions, funding organizations and research ethics boards [11]. Privacy is perceived to add yet another hurdle [4].

**Research/institutional ethics review boards** are a central part of health research governance in Canada and many Westernized countries [1;12-14]. REBs, as they are referred to in Canada, have, in general, been studied very little [6;15;16]. In terms of privacy protection, the few studies that have been conducted show that REBs demonstrate variation in requirements and decision-making practices particularly related to secondary uses of data and the proposed creation of broad-use databases [2,16,17]. Additionally, REBs themselves indicated in one of these studies that they want national guidelines related to the interface between privacy laws and the TCPS; and more detail including REB review templates. They also describe a "strong need for training of REB members in privacy and confidentiality in health research" (p.313) [16].

**Privacy advocates** are concerned that the very same technologies that bring so many new opportunities for health research also bring increased risk that disclosure of PHI may occur and that privacy may be eroded without stringent measures [10;18-20]. Some even argue that the current measures for consent, data transfer, safeguarding and security of data in health research are inadequate [10;18-20].

The **general public** appears caught in-between the above perspectives: valuing both information privacy and health research activities that require access to this highly sensitive information [4;7;21]. Careful protection of PHI is paramount because public trust and perceptions of that trust are important determinants of data quality and response rates and to reassure the public that the health research community is fulfilling its legal, ethical and policy obligations [18-24].

***Gaps in knowledge***

Yet in Canada, little is known about the exact privacy, confidentiality and security measures that are advocated by governance authorities and used in health research for both data that is stored electronically or even in paper format. Little empirical evidence exists both in Canada and internationally that provides an understanding of how health research governance authorities, i.e., REBs, protect PHI at the practice level and how they compare internationally [2;12;13;16;17;24;25]. Nor have they reviewed REB written policies in order to examine the requirements across sites [2;16]. Before future studies can determine whether these practices are adequate, or use them in policy to develop standardized procedures, the privacy, confidentiality and security measures must first be identified.

An additional gap that exists is that, in the few studies that have been conducted, none articulate the use of a conceptual framework, that guides the research and could be used for future studies [2;16].

Finally, while public opinion studies about perception of the protection of PHI in e-health systems and related to health research have been numerous over the past decade, most have not been published or made available in the public domain [26-33].

In order to address the above fundamental gaps in knowledge, the thesis had three specific objectives:

1) To identify a causal trust/risk privacy theoretical framework that will serve as a model for analyzing and predicting health research participants' privacy, confidentiality and security concerns and that will be applied to a systematic review of public opinion surveys focused on EHRs and the secondary uses of PHI.

2) To conduct a descriptive comparative analysis of international privacy best practices using the TCPS 2 and CIHR BPPP (with a particular focus on prospective broad-use databases and secondary uses of data). This will provide an understand how international standards vary in

their handling of privacy, confidentiality and information security issues, how the Canadian documents compare, as well identify any "new" practices; and

3) To identify and list Canadian FoM REBs' research protocol requirements (as indicated on their website sourced policy and application documents and with a particular focus on prospective broad-use databases and secondary uses of data) for ensuring appropriate protection of privacy, confidentiality and security of PHI in health research.

***Overview of thesis contributions***

This thesis builds on previous studies in the area of PHI protection in health research that examine international standards for protecting PHI, Canadian REB decision-making processes and the Canadian public's concerns related to privacy and PHI [2;4;7;16;17;25-28;30;32-37]. It also offers fundamental new insight, some of which, to the author's knowledge, has never been explored. These include comparing Canadian and international policy and guidance document privacy practices and examining REB policy over use of PHI in health research. **Table 6-1,** presents the key findings of each manuscript. This new knowledge provides a basis for numerous future studies as well as in the development of health research policy.

In summary, the thesis fills important gaps in knowledge and understanding in the following areas:

1) Provides a synthesis and analysis of over a decade of national Canadian public opinion surveys, largely from the unpublished grey literature and focused on the Canadian public's concerns related to the protection of PHI in the emerging EHR system and its secondary uses for health research as well as health research uses in general. Key findings show that public trust is high as it relates to primary care and with physicians protecting PHI in electronic environments. However, this trust does not transfer to secondary uses of data as in the case of health research. (**Chapter 3**);

2) Describes and compares Canadian privacy practices (as itemized from national policy and guidance documents) in health research with similar international documents. Overall, both the TCPS 2 and CIHR BPPP fair very well in comparison to similar international documents in terms of the level of detail available to the Canadian health research community related to the protection of privacy, confidentiality and security of PHI. This paper also identifies additional practices that are variation or not in the Canadian documents (**Chapter 4**);

3) Examines for the first time Canadian FoM REB written policies as available from their websites. The extracted documents provide an understanding of REB expectations regarding the protection of PHI by health researchers. This paper describes and compares REB requirements to Canadian national policy and guidance practices. Findings show that REBs do well in terms of broadly addressing the 10 privacy principles. However, heterogeneity does exist regarding the level of detail available to researchers. Once again, "new" REB practices have been identified and discussed (**Chapter 5**);

4) Provides a revised Privacy Trust-Risk Framework (much of which has been supported by this thesis) for the health research context that can be used and built upon in future studies that wish to examine the impact of advancing technologies on public trust and risk beliefs (**Chapters 2 and 3**); and

5) The findings form **Chapters 4** and **5** can be referenced and referred to by both policy stakeholders as well as privacy researchers in order to inform privacy, confidentiality and security topics that are currently being discussed and debated by the health research community.

The latter two items (4 & 5) will serve as the basis of the overall synthesis and integration of the study findings. More specifically, this chapter presents a revised model of the Trust-Risk Privacy Theoretical Framework originally presented in Chapter 2. Recently, new ideas and ways forward have been proposed in the literature in terms of actions and policies to advance the health research agenda while respecting privacy and maintaining public trust [8;10;17;38;39], such as the development of national standards and mandatory protocols

particularly in the area of data security [40;41]. Data security standards are especially important in order to increase the consistency with which REBs interpret and apply privacy protection practices in this crucial area [40;41]. Standards and/or mandatory protocols have been recommended as they also aid in the globalization of health research [40;41]. Both of these concepts have been supported by findings that emerged from this work (**Chapters 4 & 5**).

Findings from the three original thesis manuscripts will therefore be discussed in terms of their contribution towards revising the Framework and the new reforms that are presently being proposed and debated in the health research community [6;10;17;39].

## Revised Trust-Risk Privacy Theoretical Framework

The original conceptual model (**Figure 6-1**) was based on empirical studies related to the release of personal information in online e-commerce settings but never explored or supported in any other contexts including health research [23;24;42-44]. Social Contract Theory (SC) is fundamental to the Framework in that it is the basis for creating trusting beliefs that PHI will be protected [23;42;44-45]. Three areas figure prominently in terms building trust beliefs, i.e., determinants of trust: an organization's *collection* (equitable information exchange) of personal information is perceived to be fair only when the individual providing personal information is granted *control* (freedom to voice an opinion related to their rights or opt-in/out as in the concept of consent). Furthermore, the individual is informed and aware about the organization's intended use of the personal information; thus there is a *transparency* and *awareness* factor [23;42;45-49]. That is, the individual has an understanding about established conditions and practices [23;42;45-49].

As well, two additional determinants of trust are identified in the scientific literature: 1) unauthorized access to personal information that increase an individual's concerns about organizational privacy practices, i.e., decreasing trust while increasing perceptions of risk, and in contrast, 2) appropriate authorization for any secondary uses, i.e., appropriate authorization would be a factor that increases trust [50]. In **Chapter 2**, secondary uses are defined exclusively as "health research uses" from primary healthcare collections. The TCPS

2 and CIHR BPPP are cast as having a positive impact on the dimensions of SC and the determinants of trust.

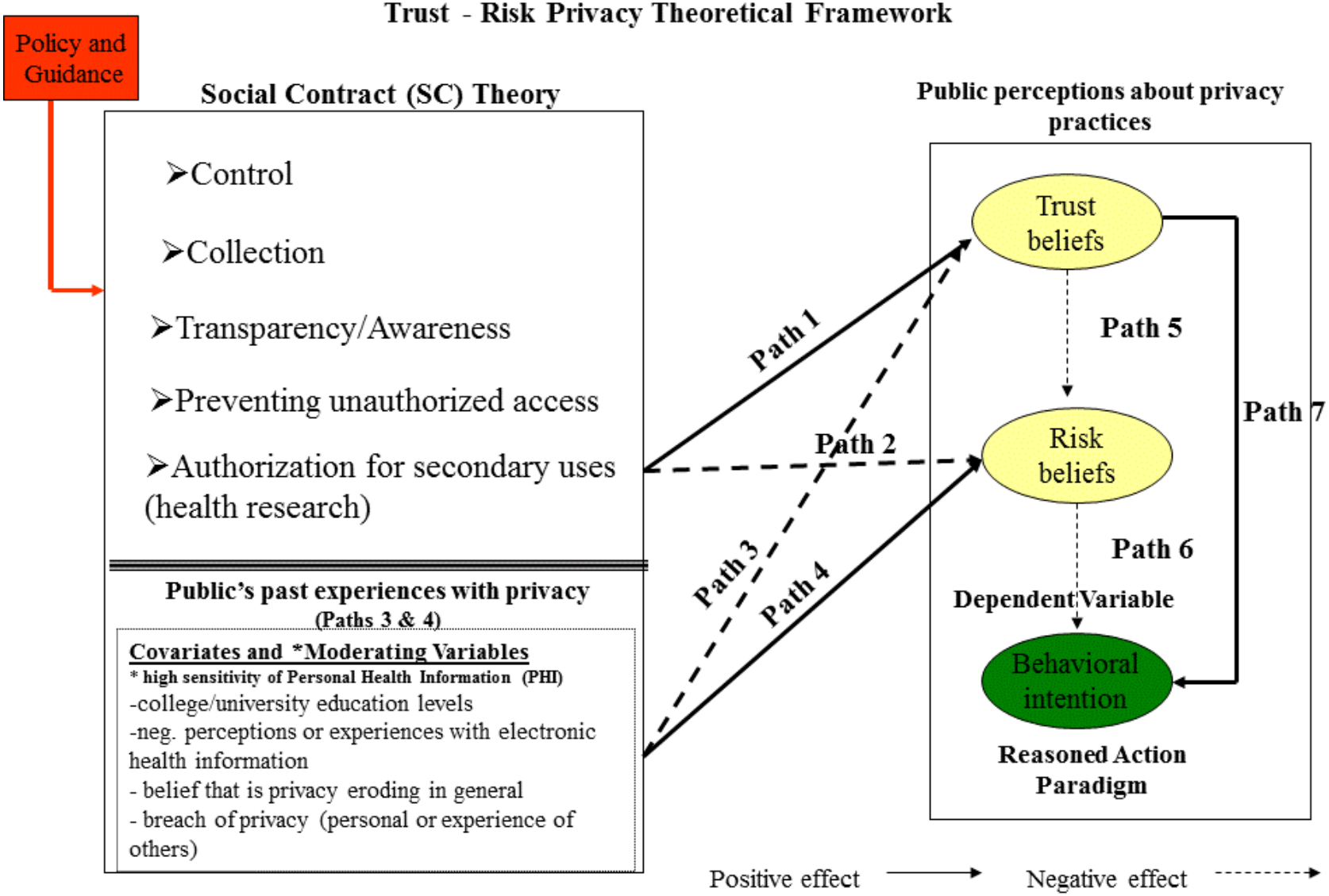
Empirical evidence from the manuscript along with new theoretical concepts from the literature can be used to inform and revise the Framework (**Figure 6-2**). To start, a careful examination of public opinion survey questions that examined preventing unauthorized access to PHI in **Chapter 3**, shows that the specific items that address this area are in fact largely *safeguards* for protecting privacy, e.g., access control measures, audit trails, strong penalties, implementation of breach management protocols [51]. The first revision to the Framework is therefore highlighting "safeguards" as a key determinant of trust and risk beliefs.

**Chapter 3** also offers interesting insight and comparison between the trust the Canadian public has with physicians versus health researchers and the consequences related to consent [51]. In terms of physicians, results show that the public trusts primary care physicians and other professionals within the circle of care [51]. In fact, public trust that physicians will keep PHI safe and secure does not fall below 86% in national surveys [30]. In contrast, trust that health researchers will do the same is significantly lower: health researchers in universities (57% 2004; 52% 2007), government health researchers (54% 2004; 52% 2007), private sector health researchers (46% 2004; 45% 2007) [30]. This is despite the fact that health researchers typically have access to data that does not contain nearly the amount of PHI in terms of quantity and detail as physicians [4;21;25].

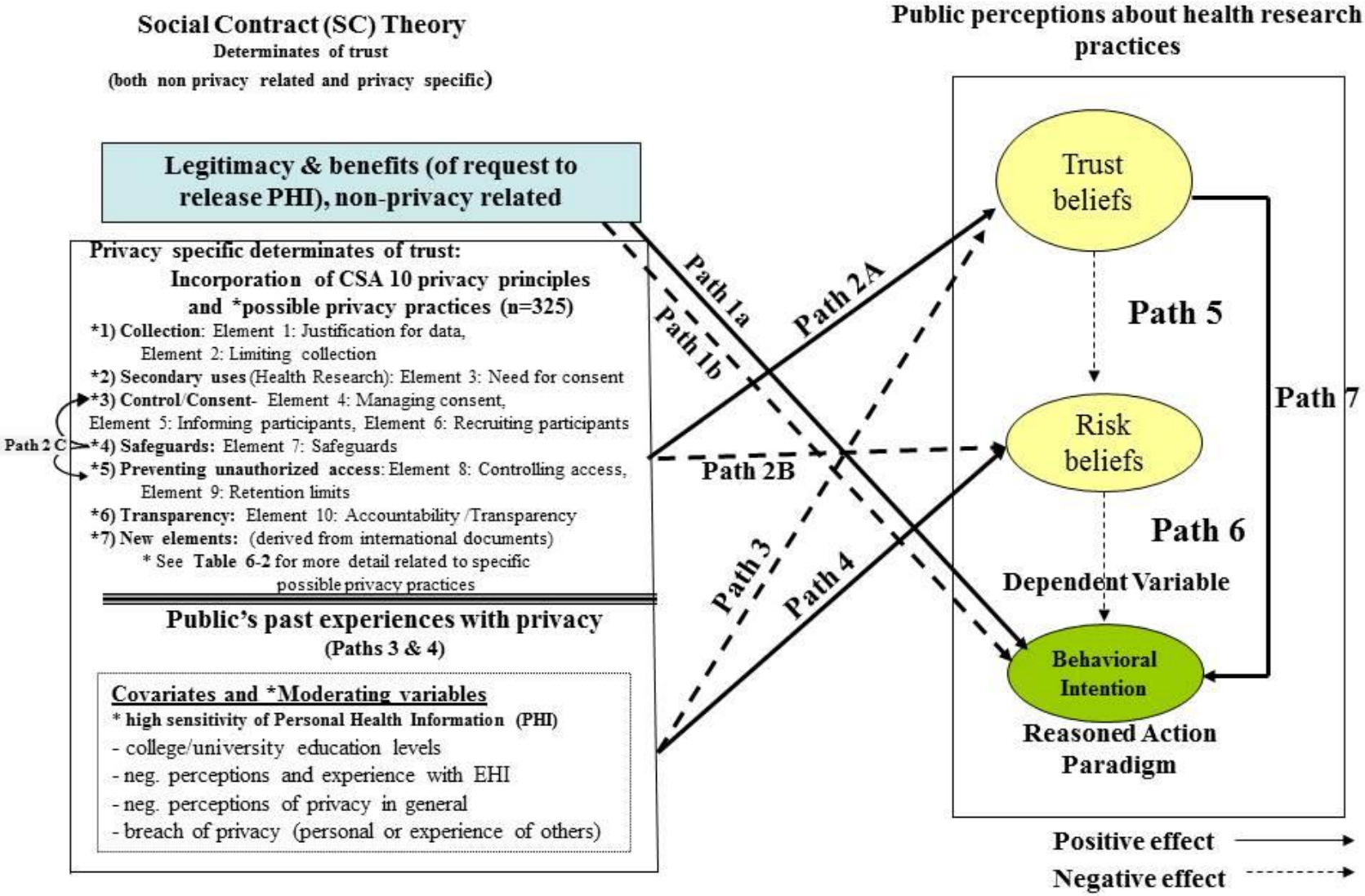
In contrast to secondary uses for health research purposes, it is interesting to note that the public is largely comfortable with secondary uses of their PHI by administrators of the health-care system without their expressed consent, e.g., to address public health issues 71%; 2007 [30]; to plan, monitor and evaluate the health-care system (74%; 2007); to prevent improper use of the health-care system (71%; 2007). These results have also been confirmed by other studies that show that using PHI to improve quality care (86%, 2007) and to track communicable diseases (89%, 2007) is acceptable [7]. The reason for this divergence in view is not clear.

## Figure 6-1

**Trust - Risk Privacy Theoretical Framework**



## Figure 6-2
**Revised Trust - Risk Privacy Theoretical Framework**



Consequently, "implied" consent was identified by the public to be sufficient for physicians and other health-care providers to share PHI within the circle of care, as well as the examples of system administration and surveillance provided above. However, "implied" does not transfer to the release of PHI for health research purposes even if data has been stripped of direct identifies first [51]. The public therefore appears reluctant to completely delegate trust to health researchers and to reduce or waive consent requirements for lower-risk de-identified studies [51]. Of significance to the Framework is this data supported **Paths 5** and **6** in **Figure 6-2**, by demonstrating the role of trust and risk beliefs in terms of the intention to release PHI by the public.

Conversely, a majority of Canadian do not automatically authorize many secondary uses of their PHI, even internal uses, such as in hospital fundraising activities 62%, 2004) or spiritual counselors, e.g., hospital chaplain (78%, 2004) without their express consent [40]. These examples provide evidence that the concept of *collection* must be viewed as a fair exchange. That is, the public will release their PHI for primary and secondary uses if the purpose is perceived as "legitimate". It does not necessarily need to lead to direct benefits for the individual, but there is a sense by that person of a perceived benefit in some way which is of value [31;50]. The examples also show that some of the uses of PHI have different outcomes in terms of trust, e.g., primary care versus hospital fundraising and hospital chaplaincy, even if they occur within the same environment with the same privacy, confidentiality and security measures. Therefore, PHI protection measures may be irrelevant if the individual fails to see the legitimate purpose or benefits to themselves or society [51]. Previous studies also supported the concept of "legitimacy" and "benefits" of the exchange as a key factor that determines whether an individual will provide their PHI [52]. Therefore, *Legitimacy and benefits* is cast as a separate and initial starting point for trust that has a direct bearing on "Behavioral intentions to release PHI" that does not necessarily relate to privacy determinants. Therefore, if a research initiative demonstrates and even surpasses all privacy, confidentiality and security expectations of the potential participant, it does not mean that the individual will participate, **Figure 6-2: Path 1b**-negative impact scenario). On the other hand, if a study seems highly important and particularly relevant to a prospective research participants, it is also possible the individual may participate in the study regardless of the

privacy practices since *Legitimacy and benefits* are not been directly linked to trust, e.g., terminal cancer patient participating in a clinical trial for an new treatment approach, **Figure 6-2: Path 1a** -positive impact scenario) [52]. This path suggests that some research participants can be particularly vulnerable as the strong desire for a particular benefit may mean the research participant neglects or pays little attention to the other factors at play such as privacy protection. Further study of this variable is needed to better understand its overall role in the public's decision-making process and specifically if the public is willing to overlook privacy in certain health research scenarios that may not have agreed to at other times.

***Consent conceptualized as "entrusting"***

William H. Lowrance, an international health policy and ethics scholar, radically challenges the current notions of consent in health research In his book, *Privacy, Confidentiality and Health Research* (published in 2012 by Cambridge University Press), [10].

The Framework casts consent as part of the *control* determinant. It specifically adopts the definition that emphasizes the idea of "free and voluntary" participation in health-care or health research [14;53;54]. Canadian privacy practices emphasize informed and ongoing consent through the use of consent forms and/or notification [14;53;54]. However, according to Lowrance, the particular notion that the reliance on "informedconsent" [sic] as the catchphrase goes, as an indicator that a participant comprehends in some depth the research purposes and plans, the information security measures, the compliance with laws and regulations, the risks to privacy and confidentiality, and so on, and that signing a consent for serves autonomy, can amount to a charade" (p. 85)[10]. He goes further to say that "the most serious ethical fallacy is when consent is posed as empowering people to "control" the use of "their" data or biospecimens that are not really theirs in any strong sense in the first place. These limitations must be faced and polices rethought" (p.85)[10]. Are these views accurate? Are the concepts of "consent" and "control" as they have been thought of to date merely "ethical fallacies" as Lowrance describes them?

The evidence from the **Chapter 3** in particular does not completely support Lowrance's view. Instead, it shows that in the context of health research the public does understand and desire the traditional definition of consent as part of "control" [51]. Furthermore, it also shows that the public is not willing to give this up even if direct identifiers are not used in health research activities [51]. But the public is prepared to relinquish "informed consent" as it is currently defined in direct healthcare scenarios within the circle of care [51].

Lowrance concludes that "realistically, what should be sought in health research is general understanding of a project's purposes, procedures, and risks, in as much depth as prospective research participants' want, and then informed deference to the project's setting, leadership safeguards, and governance, i.e., *consent construed as entrusting*—which is what consenting often amounts to in reality" (p.86) [10]. He cautions the reader that an important condition before considering this (or any of his reforms is)"assuming in each case that proper safeguards are maintained and robust governance is exerted" (p.86) [10]. Adequate confidentiality levels and proper safeguards through the use of standards and certification processes along with a proportional approach to privacy risk management is strongly advocated by many researchers including Lowrance [3;10;17]. Lowrance highlights the fact that concerns about security of electronic data had been identified as a factor that the public says "most strongly discourages them from agreeing to participate in research" (p. 131) [10]. As such, assuring the public that adequate confidentiality levels and security practices are in place is key in helping to "make trusting reliable" (p.86) [10].

While the idea that meaningful consent (and *control*) in health research is not fully examined, this thesis is notable in that it does provide evidence to view consent as "entrusting" particularly in the primary care e-health context. Specifically the concepts that have been espoused for Figure 2: Path 2 A&B that determinants such as *control, preventing unauthorized access, safeguards, transparency/awareness* and *collection* all promote trust (or the lack thereof which then leads to perceptions of risk) are supported by **Chapter 3**.

**Chapter 3** provides evidence that while the public is capable of viewing consent as "entrusting PHI" particularly in terms of primary care, if trust is low, so is the mood for

reducing or waiving consent in the secondary uses of PHI for health research purposes. Therefore, if the health research community wants the public to embrace the concept of consent defined by Lowrance, then more work is needed, particularly in terms of strengthening the determinants of trust starting with "Security Safeguards".

To more clearly expand on this concept, in **Figure 6-2**, consent is now presented as going hand-in-hand with *control*. Therefore the concept of *consent* is redefined according to Lowrance essentially as authorization to proceed based on trust in researcher and organizational practices that mitigate privacy risks most notable safeguards and an understanding of the projects purposes [10]. This definition casts consent (and therefore *control*) as being directly influenced by *safeguards*. *Preventing unauthorized access* remains influenced by *Safeguards*, **Figure 6-2: Path 2C**.

**Chapter 3** also shows that the use of security safeguards to prevent unauthorized access (including: adherence by staff to strict security protocols; access control measures; and severe penalties for unauthorized access) are all strongly desired by the public [55]. Appropriate safeguards are therefore critical and cannot be omitted when discussing strategies for building public trust [10;51]. While the concept of a security "certification process" does not directly emerge from this paper as it did from Paper 3 (**Chapter 5**), it makes sense that being able to demonstrate to the public that information and communication systems meet a rigorous standard would be a facilitator of trust [10].

In summary, findings from **Chapter 3** related to the publics' needs regarding health research data privacy, confidentiality and security include:

1) Use of notices, brochures and pamphlets in doctors' offices would be a welcomed way of informing the public regarding secondary uses of PHI as well as accountability mechanisms.
2) Application of security safeguards including: that all those with access to PHI adhere to security safeguards; access control measures and audit trails; and be subject to strong

penalties for unauthorized access. Breach notification; accessible privacy policies; and implementation of breach management protocols were also desired.

3) Public requirement for some type of consent or at least notification for secondary uses in health research, even if data has been stripped of direct identifiers [51].

Given the latter requirement, ongoing public engagement is needed in order to adequately address the public's concerns. Achieving meaningful public dialogue will encourage support and awareness about the use of PHI in health research contexts and in so doing, build public trust [4;8;55].

Strengthening safeguards as well as other practices related to *collection, control, preventing unauthorized access, safeguards* and *transparency/awareness* is shown in **Chapter 3** to be instrumental in enhancing trust while reducing perceptions of risk. Therefore, it is important to first identify the privacy, confidentiality and security practices that are currently used by Canadian and international governance regimes, in order to identify a baseline of practices from which to start, and also to develop harmonized privacy standards in health research toward *making trusting reliable* [10].

A 2007 citizens' dialogue confirms that a system of checks and balances will allow the public to have confidence and trust in how PHI is managed in the health research context [50]. Both the TCPS 2 and CIHR BPPP are therefore cast as having a positive impact on the dimension of *Authorization for Health Research*. Specifically, the 10 CSA privacy principles are presented as the overarching determinants of trust, given their similarities to *control, collection, preventing unauthorized access* and *security* (see **Table 6-2**). Consistent with the e-commerce framework, positive impacts on the SC dimensions build research participant trust **(Path 2 A & 2C)** and decrease risk beliefs **(Path 2B)**. However, the remaining two manuscripts (**Chapters 4 & 5**) do not set out to prove, disprove or identify which of the 10 CSA privacy principles or specific privacy practices (total n= 325 privacy practices) have more or less impact on trust and risk (**Table 6-2**). Further study is required to better understand the roles that the principles and the practices in terms impact on trust and risk beliefs.

## Table 6-1: Summary of objectives and manuscript findings

Guiding theoretical framework: **Trust-Risk Privacy Theoretical Framework**

| Study | Objectives | Methods | Main findings | Key contributions |
|---|---|---|---|---|
| **1. Canadians' opinion on privacy and electronic health information (2000-2012)** | The systematic review is designed to address several research questions: 1) What is the public opinion and experience regarding personal health information privacy and EHRs (according to the six dimensions of the Trust -Risk Privacy Framework)?<br><br>2) How much does the public trust physicians and health researchers to keep their personal health information safe and secure in EHR environments? And<br><br>3) What is the public opinion regarding privacy and access to personal health information for health research through the EHRs? | A formal systematic review was conducted from 2000-2012 including a comprehensive review of the unpublished grey literature, e.g., custom and syndicated stakeholder studies.<br><br>Trends in six outcomes include public concerns over personal health information (PHI): 1) control; 2) collection; 3) transparency & awareness; 4) unauthorized access; 5) authorization for health research; and 6) trust and risk beliefs. | 1) Sixteen unique surveys totaling responses of over 20,000 adult Canadians show that the public values both the potential of EHR systems, health research activities and maintaining the privacy of their PHI. Their views are strong and optimistic.<br><br>Canadians trust their health-care providers. This trust, in conjunction with low levels of reported incidences involving PHI, drives high comfort levels with electronic information sharing between health-care providers within the circle of care.<br><br>This high comfort and confidence does not automatically extend to health researchers or the secondary use of PHI for health research, even if data has been de-identified first.<br><br>The survey results largely reflect perceptions about EHRs and not experiences. | The findings support strong policy and practice related to PHI protection and caution when considering different consent models related to the secondary uses of health research. |

| Study | Objectives | Methods | Main findings | Key contributions |
|---|---|---|---|---|
| **2. A Descriptive Comparison of International and Canadian Guidelines in Health Research Privacy** | 1) Provide a current literature review and comparative analysis of international FIPs.<br><br>2) a) Identify and conduct a descriptive content and item-by-item comparative study of international health guidance and policy documents with similar Canadian documents and identify the documents that were:<br>i) Specific to privacy protection or health research practices in general;<br>ii. Broader ethics principles or FIPs (or both).<br><br>b) Conduct a descriptive comparative study of the international document to Canadian health research policy and guidance documents with particular attention paid to provisions related to primary and secondary uses of data and the establishment of prospective data bases for broad use in research; and<br><br>c) Create a listing of privacy protection items derived from the international documents not covered by the Canadian documents | The research proceeded through five phases leading to both qualitative exploration and quantitative content analysis of relevant documents available in the public domain. Documents were searched from an unspecified start date to October 01, 2010 and updated April 2, 2013.<br><br>The TCPS 2 and CIHR BPPP document privacy practices were combined into a 162 item list. The content of the 162 item list was then independently verified. The resulting combined list served as the template for the international item-by-item comparative analysis. | 1) Six international FIPs were compared and are found to share most of the core eight-10 principles.<br><br>2-3) Twenty-eight international guidance documents were identified. Those that were derived from both FIPs and ethics principles (five of 28) show the greatest commonalities in terms of best practice items and were most likely to be specific to health research privacy.<br><br>The comparative content analysis with the combined list of 162 items shows that the 70% of the content of 24 of 28 documents mirrors privacy practices found in either the TCPS2 or CIHR BPPP.<br><br>4) 100 additional potential privacy protection practices emerged. | • Ethics principles (as opposed to FIPs) form the foundation of most guidance documents.<br><br>• Ethics principles are found to be less comprehensive at protecting privacy.<br><br>• The Canadian TCPS2 and CIHR BPPP documents are similar to international privacy protection documents and offer highly comprehensive privacy guidance.<br><br>• The unique elements emphasize current concerns regarding protecting electronic health information, i.e., de-identification; anonimization; legislation; and proportional approach to privacy protection |

| Study | Objectives | Methods | Main findings | Key contributions |
|---|---|---|---|---|
| **3. What are Canadian University Biomedical Research Ethics Board (REB) Requirements for Protecting Privacy? A Descriptive Review of REB Policy and Website Guidance Documents.** | 1) To assess the privacy protection requirements of Canadian university biomedical faculty of medicine (FoM) REBs against those found in policy (mandatory) and guidance (elective) documents available in Canada.<br><br>2) To assess the privacy protection practices of FoM REBs in three areas relevant to advancing technologies: waiver of consent requirement for the secondary uses of data; creation of prospective data bases for general use; and the use of a "risk assessment and proportional management" strategy to protecting privacy against both policy and guidance practices in these areas.<br><br>3) To identify other REB privacy practices regarding the protection of privacy, confidentiality, and security of PHI as required by FoM REB website research protocols. | A list of 17 faculties of medicine (FoM) in Canada was obtained from the Association of Faculties of Medicine of Canada (AFMC). All FoM REBs were included for consideration.<br><br>The TCPS 2 and CIHP BPPP combined 162 privacy practice items was used to conduct the comparative analysis.<br><br>All documents related to full board review, i.e., REB policy and research protocol including templates were extracted and compiled from each eligible REB website<br><br>A coder reproduced a sample of 15% of the document analysis. | Fourteen of 17 FoM REBs met the inclusion criteria<br><br>1) All REBs indicate compliance with the TCPS 2. Four of 14 recommend or reference the CIHR BPPP<br><br>Almost all REBs (13/14) address all of the 10 privacy principles in some way.<br><br>Inclusion of TCPS 2 items ranges from 38%-97% across REBs; for items from the combined list of TCPS2 & CIHR BPPP and for that CIHR BPPP inclusion ranges from 25%-77%.<br><br>2) All REBs address secondary use in some way; 11 of 14 address general-use database practices with low uniformity across REBs. 14 REBs state a need a proportional privacy risk management approach.<br><br>3) While REBs have demonstrated innovative approaches to privacy protection particularly in terms of electronic data (63 additional were identified), the largest number of additional practices (15) relates to safeguarding data. | • This study represents the first time that REBs web based privacy protection documents have been examined.<br><br>• Study findings echo previous studies that show high variability in practices across REBs (inclusion of TCPS 2 items is noted to be higher).<br><br>• The highest uniformity is seen in the secondary use element; yet previous studies show that this element has high decision-making variability. This suggests that more research is required to understand REB needs in this area.<br><br>• Prospective use databases is an area where there is by REBs to fill gaps noted in the TCPS 2; again suggesting that REBs require more guidance in this area.<br><br>• Safeguards and a proportional approach to privacy risk management are noted to be lacking in detail in policy, guidance as well as REB requirements. |

**Table 6-2: Trust Risk Conceptual Framework: determinants of trust and possible privacy practices**

Original Framework elements matched to the CSA 10 Privacy Principles including all possible*****privacy practices (**n=336 total possible privacy practices**)

| **Original Framework elements** | **10 privacy elements + new elements** | **Privacy practices: TCPS 2 + CIHR BPPP (n=162)** | **Privacy practices: International (n=100)** | **Privacy practices: Canadian FoM REBs (n=63)** |
|---|---|---|---|---|
| **1) Collection** (*Total possible privacy practices: **47**) | -Data needs are justified according to research objectives | 12 | 3 | |
| | -Limiting collection of PHI | 12 | 7 | 13 |
| **2) Secondary uses (Health research)** (*Total possible privacy practices: **26**) | -Determining if consent is required | 17 | 6 | 3 |
| **3) Control/consent** (*Total possible privacy practices: **108**) | -Managing and documenting consent | 8 | 3 | |
| | -Informing prospective participants about the research | 45 | 26 | 5 |
| | -Recruiting prospective research participants | 13 | 8 | |

| **Original Framework elements** | **10 privacy elements + new elements** | **Privacy practices: TCPS 2 + CIHR BPPP (n=162)** | **Privacy practices: International (n=100)** | **Privacy practices: Canadian FoM REBs (n=63)** |
|---|---|---|---|---|
| **4) Security safeguards** (*Total possible privacy practices: **60**) | -Safeguarding PHI | 28 | 15 | 17 |
| **5) Preventing unauthorized Access** (*Total possible privacy practices: **47**) | - Controlling access and disclosure of personal data | 9 | 8 | 17 |
| | -Setting reasonable limits on retention of personal data | 8 | 3 | 2 |
| **6) Transparency and Awareness** (*Total possible privacy practices: **22**) | -Ensuring accountability and transparency | 10 | 6 | 6 |
| **7) New elements** (**international**) (*Total possible privacy practices: **15**) | -Requirements for data to be "truly anonymous"<br>-Privacy protection for anonymized data<br>-Demonstrating compliance with privacy legislation<br>-Capacity for consent procedures<br>-Describe "proportionate approach" to protecting privacy | | (total) 15 | |

*** Note:** It is the specific possible privacy practices that may be useful in the development of proportional and standardized practices.

***Summary***

The revised Framework (**Figure 6-2**) is derived from and integrated with empirical evidence from this manuscript as well as from new theoretical concepts currently being proposed in the academic literature related to privacy risk and participation in health research. While the original Framework was informed primarily by Social Contract Theory and Reasoned Action Paradigm and conceptualization of trust beliefs and risk beliefs, a major limitation was that empirical evidence to support the original Framework was derived solely from the e-commerce sector.

The revised Framework builds on the original model and represents an integration of empirical and theoretical evidence directly from the health research context internationally and in Canada. It continues to emphasize the importance of trust and risk beliefs, but highlights the following elements and their impact of facilitating trust:

- *Legitimacy and benefits*, emerging from **Chapter 3** as well as the literature (originally part of *collection* as a fair and reasonable exchange) is now cast as the first step prior to an individual's consideration of whether or not to participate in health research and is not necessarily influenced by trust and risk beliefs.
- *Consent* now goes hand-in-hand with *control*. This was done to clearly show the importance of an individual's authorization to proceed (*consen*t) as singularly important to providing a sense of *control* over PHI when "entrusting" to health researchers.
- *Safeguards* has been isolated from *preventing unauthorized access* but is noted to influence it. This highlights the importance of adequate *safeguards* for ultimately influencing trust and risk beliefs.

The above conceptualizations are supported in large part by findings from **Chapter 3** and are also informed by new thinking on this topic recently introduced in the literature.

**Privacy governance in health research: harmonization and standardization as a way forward**

**Chapter 4** provides a comparison of Canadian health research policy and guidance documents with similar international ethics and privacy documents and identifies all additional practices not present in the Canadian context. In order to conduct this review, the CIHR BPPP (the more detailed of the two documents) was first converted to a list form that would allow for a systematic comparison. The TCPS 2 policy document was them mapped to the CIHR BPPP and additional practice items were added to produce a master list of 162 practices. Using this master list, results show that the TCPS 2 and CIHR BPPP, derived from FIPs and ethics principles, offer a comprehensive guide to privacy protection that compares well to the international documents [40].

In **Chapter 4**, a total of in 100 privacy protection practices are identified that are either variations of those found in the combined list of practice items from the Canadian documents or completely unique to them [40]. As well, three new elements with 11 privacy protection practices emerge(**Table 6-3**) [44].

**Table 6-3: New privacy practices identified from the international documents and not included in either the TCPS 2 or CIHR BPPP (Chapter 4)**

| Element No. | Description | No. of items/practices |
|---|---|---|
| **1** | **Identify requirements for data to be deemed "truly anonymous" and requirements for using or sharing such data.** | 7 |
| **2** | **Acknowledge difficulty in truly anonymizing data; identify privacy protection for anonymized data.** | 2 |
| **3** | **Demonstrate compliance with relevant privacy legislation and provide notice of said legislation to participants.** | 2 |

A fourth element (not presented in the table), while not new to either the TCPS 2 or CIHR BPPP is mentioned due to relative importance and lack of detail in either Canadian document [40]. This fourth element is noteworthy as it highlights the need for proportionality when managing privacy risk, particularly in terms of safeguarding PHI [40]. While this concept is expressed in both the TCPS 2 and CIHR BPPP exactly how this is to be done is not expanded on in these documents. While two of the international documents ask researchers to provide detail regarding this item, the documents themselves offer very little direction in terms of how to apply a proportional approach [40].

A complete list of all possible practices can be generated by combining the list of 162 privacy practices derived from the TCPS 2 and CIHR BPPP, the 100 additional practices from the international documents and 63 practices from Canadian REBs (n=325 possible privacy practices) (**Table 6-2**). Once the 163 additional practices have undergone review by subject matter experts to determine appropriateness, the expert panel reviewed list can be used in the development of privacy standards that have the added advantage of being consistent with those found internationally [40;41]

**Chapter 5** examines local governance practices, focusing on how Canadian REBs reflect and capture the combined list of items on their website research protocol requirements, i.e., forms and policies. To the author's knowledge, the thesis represents the first time that Canadian university FoM biomedical REB website research protocol requirements have been examined to see how they are ensuring that personal information is protected in health research protocols. While the paper reveals relatively high REB compliance with core privacy principles, it also shows relatively high variability across FoM REB website policy and application documents [41].

However, findings also indicate that consistency in forms and policies does not necessarily lead to more consistent decision-making amongst REBs [41]. For instance, the secondary uses of PHI, which present the least variability of privacy protection practices, are shown by previous studies to display low consistency in decision-making practices across REBs [16]. Additional highly relevant "best practices" exist for the secondary uses of PHI currently exist, but REBs do not reference or use them [41]. Further study to understand why this is the case would prove helpful when developing future best practice documents.

Safeguard requirements for protecting data is an area that shows a lower inclusion of items [41]. In addition, it shows a variation both in terms of inclusion of the combined items, as well as TCPS 2 requirements in both the number of types of items. This finding confirms previous studies that have examined this area [16]. Interestingly, safeguarding data is also one of the areas with the largest number of innovative practices [41]. This suggests that, with the threats to privacy posed by advancing technologies, REBs may be struggling to understand which safeguards to implement to protect data security [41]. In support of this position, the few high profile privacy breaches in health research that have been reported in the media over the last few years point to inadequate safeguards as the primary cause [56;57]. Given the importance of safeguards as determinants of trust, adequate safeguards warrant a great deal of attention by the health research community [10;51].

The last finding observes that, while both the TCPS 2 and CIHR BPPP advocate a proportional approach to privacy risk management, they are relatively silent as to how REBs and researchers should go about doing this [41]. As such, it is not surprising that REBs are also silent on this matter [41]. The findings confirm a need for the development of proportional and harmonized standards [41].

Where standards do not currently exist, they could be derived from the combined list of 162 practices from the TCPS 2 & CIHR BPPP, and the additional international documents, as well as the new REB practices. Where standards do exist, i.e., ISO 27002, certification would be used to demonstrate system conformance [10]. More specifically, the certification process would be confirmation that the privacy and security policies, procedures and practices at the research site meet the standards [8,55].

Advantages of creating and using standards are numerous: for researchers they include a clear and harmonized understanding of privacy protection requirements, while the burden on REBs would be reduced as the need to assess data and privacy protection practices would be lessened [60]. National standards and certification would offer a transparent and accountable method to build and maintain public trust that PHI is protected in health research contexts [25;55].

***Interrelationship of the three manuscripts***

A review of the compellation of survey questions and responses (**Chapter 3: Table 3-3**) shows that most of the questions and responses (17) related to the combined principles of safeguards and preventing unauthorized access followed by the principle of limiting collection (12 questions/responses) [51]. Coincidentally, this observation exactly mirrors the order the privacy principles emerged according to the grouping of the 63 additional items for the REBs and also aligns very closely to findings from the comparable international guidance documents [41;40]. It appears that, in today's environment, the public, REBs and the international health research community have similar priorities in terms if protection of PHI. Specifically, all three emphasize safeguards. The Canadian public highlights the need for preventing unauthorized access/safeguards including malicious unauthorized access,

unauthorized uses and human error [51]. Enhanced measures in this area are desired and include: staff must adhere to stringent measures; access control; audit trails and strong penalties [51]. While the TCPS 2 does not provide the level of detail the public is calling for, the CIHR BPPP does (**Appendix 1**). As well, the additional items derived from both the international context and REBs further complete the picture for what the public is wanting [41;40]. **Chapters 4 & 5** therefore specifically provide measures for addressing the Canadian publics concerns related to PHI protecting in health research [41;40;51].

***Summary***

Introducing certification of safeguards and standardization of privacy practices which are largely derived from the TCPS 2, CIHR BPPP and new items from the review of the international privacy protection documents and Canadian REB practices provides the starting point for a pragmatic proportional risk management approach. This type of approach is increasing supported in the literature as a way forward to managing the heterogeneity of current privacy practices [3;10;17]. Most importantly, it addresses the publics privacy protection concerns related to electronic health information.

## Implications for population health

This thesis provides further empirical evidence that the public's negative perceptions of personal data privacy can reduce trust and participation in health research [51].

EHRs, along with broad-use databases, facilitate clinical and population-based health research, monitoring and surveillance using PHI data [58]. Secondary uses of PHI from EHR systems have the potential to accumulate an individual's lifetime personal health information (including the broader factors that influence health status, e.g., socio-economic conditions, education, culture, literacy). This "cradle-to-grave" information would be invaluable for clinical and population health research, monitoring and surveillance [18;59].

It is particularly timely to understanding the public's perception about privacy in the health-care context in general and regarding health research specifically, and determining whether the health research community's systems to engender public trust are adequate, given advancing technologies. Outcomes from this study can be used: to develop more systematic approaches to protecting privacy in population health research; to audit information use practices and safeguards; to establish and strengthen reporting relationships to the Information/Privacy Commissioner; and to meet the Canadian public's expectation that concrete steps are being taken to protect personal health information privacy, security and confidentiality in health research contexts [4;7;16;23;25;50].

Specifically, the findings from this work can be applied to health policy in the following ways:

1) assist in the development of proportional model for privacy protection in health research;

2) emulate or avoid additional privacy practices identified in the international documents and REBs in future revisions of the TCPS or CIHR BPPP documents;

3) inform establishment of standards to assist REBs in evaluating protocols that use PHI, and promote consistency across the country and build towards a standardized and harmonized approach;

4) assist health researchers in implementing appropriate privacy, confidentiality and security safeguards; and

5) establish a baseline mechanism that can be used for auditing members of the health research community including researchers, research organizations, institutes, facilities and REBs, in terms of minimum standards regarding the privacy, confidentiality and security of PHI.

**Implications for future research**

The concepts identified by the original manuscripts as well as the final conceptual Framework raise a number of specific questions for future research:

1) Findings from Chapter 3 show that the public values health research in general. However, there is a need to examine the specific factors (outside of privacy) that lead the public to view health research activities as legitimate and beneficial and therefore important for participating in;

2) There is a need to further examine the specific types of "control" and health research governance mechanisms that promote trustworthiness and lead to authorization by the public to participate in health research, particularly in terms of secondary uses of PHI and broad-use databases. Furthermore, the most appropriate methodology (that complements and expands on public opinion surveys) for obtaining meaningful and in-depth results given the complexities of the issues being discussed must be decided upon;

3) The list of new practices identified from the international documents (n=100) and FoM REBs (n=63) require a review of the items to confirm which ones are truly unique and appropriate for inclusion as part of recommended practices for researchers. An eDelphi approach using subject matter experts represents one methodology that can be useful in this review.

4) The total list of items, that is, the combined TCPS 2 and CIHR BPPP as well as unique practices confirmed from the previous step, i.e., reduced based on review by subject matter experts, can be structured into an online proportional risk management approach. Such an approach would guide researchers towards the optimal privacy protection practices given the identifiable nature, sensitivity, format (paper or electronic) and amount of data being collected as well as other risks, such as need for portability. The eDelphi methodology privacy and security subject matter experts could

also be useful as respondents would be asked to group and rank items in term of importance.

5) Further study of the Framework is needed to better understand the role of the TCPS 2 and CIHR BPPP (and their specific privacy practices) as well as the specific additional practices from the international documents and FoM REBs in building meaningful public trust that PHI is protected in the health research context.

## Limitations of the research

***Limits to reliability, validity and generalizability:***

Several limits to reliability and validity have been mentioned in the papers and some will be expanded on and highlighted here.

In the first manuscript (**Chapter 3**) survey reliability and validity results were typically not reported and could not be ascertained.

Next, the grouping of survey questions according to the six dimensions of the Trust-Risk Theoretical Privacy Framework could only be done subjectively as objective guidelines or protocols do not exist regarding the dimensions. However, replication of the selection and grouping of the questions would greatly add to both the reproducibility and assurance that the questions reflect the dimensions they are intended to.

In the second manuscript (**Chapter 4)**, the collection of international documents and their comparative analysis with the Canadian documents provides significant insight. However, as it was limited to document analysis, it did not include input from the documents' authors, health researchers or research ethics review boards. Interpretation of the documents was therefore left to the study author. This could have resulted in the misinterpretation of criteria when abstracting data (thus affecting both the reliability and validity of findings). As well, input from these key stakeholder groups would have provided interesting ideas regarding the guidance document usability and interpretation. However, use of a second data abstractor (PM) helped offset this limitation.

In addition, the TCPS 2 list of items did not benefit from verification by an independent party as did the CIHR BPPP item list. This also increased the risk of possible misclassification of items.

In the third manuscript (**Chapter 5**), it is not known whether REBs use more privacy items and considerations than just those listed in their website documents when reviewing research protocols. Specifically, it may mean that additional REB review processes that could have offered more insight into the requirements of research protocols, without input from REB members or researchers, have been omitted. The findings likely represent the minimum requirements of REBs. However, as previous studies have utilized qualitative methodologies and have focused on the decision making process with similar findings, this study serves to corroborate the previous results.

Other limitations identified include:

- Two REBs whose website documents could not be accessed (due to restricted requirements in the public domain) and could potentially have privacy requirements that differ from those that are in the public domain. Generalizability to all university faculty of medicine REBs is therefore limited.
- Focusing on only one population of REBs limits any generalizability of results. Including more categories of REBs, and in particular, those that deal with sensitive PHI, e.g., mental health institutions, hospital-based REBs or REBs that review protocols primarily for vulnerable populations such as pediatric institutions and the elderly) would provide significant insight into how these REBs protect PHI given the added risks to privacy involved. Additionally, including human biological materials, review of genetic protocols and other highly complex topics will add significantly to the understanding of REBs' decision-making in these complex areas.

The Trust-Risk Privacy Theoretical Framework offers a paradigm to understand how privacy protection measures can impact the public's trust and risk beliefs when providing PHI in the research context; however, it does not provide sufficient detail to explain which privacy

protection items should be included and can have the most impact at minimizing privacy risks and maximizing trust. As well, its lack of specificity in the health research context also limits the overall guidance it can offer. One suggested method to address this issue is to use the "combined list" of items from the TCPS 2 and CIHR BPPP. Future studies utilizing the Framework in health research contexts would greatly add to the Framework's applicability to the health research context.

## Conclusion

In summary, the three original manuscripts individually produced new knowledge related to the research questions asked, as well as provided specific policy implications that enhance the public's trust related to privacy protection in health research. They offer a foundation that can be built upon towards the harmonization and standardization of privacy practices. They also provide empirical evidence which, along with new theoretical ideas, support a revised Trust-Risk Privacy Framework (**Figure 6-2**). The revised Framework can be referenced and used to inform privacy issues faced by the health research community.

The thesis findings offer a pragmatic platform for discussion, future research ideas and policy direction aimed at demonstrating to the public that PHI entrusted to health researchers will be carefully protected.

## REFERENCES

(1) Canadian Institutes of Health Research (CIHR). Selected International Legal Norms on the Protection of Personal Information in Health Research. 2001.

(2) Gibson E, Brazi K, Coughlin MD, Emerson C, Fournier F, Schwartz L. **Who's minding the shop? The role of Canadian research ethics boards in the creation and uses of registries and biobanks.** *BioMed Central Medical Ethics* 2008;**9(**17):1-9. Date accessed 11/04/2011. www.biomedcentral.com/1472-6939/9/17

(3) Slaughter PM, Collins PK, Roos N, Weisbaum KM, Hirtle M, Williams J.. Privacy Best Practices for Secondary Data Use; Harmonizing Research & Privacy: Standards for a Collaborative Future. Privacy Best Practices for Secondary Data Use (SDU) [CD-ROM] 2006.

(4) Willison DJ. **Privacy and the secondary use of data for health research: experience in Canada and suggested directions forward.** *Journal of Health Services Research and Policy* 2003;**8**(1):S1:17-S1:23.

(5) Straf M. Forward. In: Doyle P., Lane JI, Theeuwes JJM, Zayatz LV, Editors. *Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for statistical Agencies.* Amsterdam: Elsevier Science B.V.; 2001. p. ix-x.

(6) Flood CM, Thomas B. **Searching for a sweet spot: How do we trade off research benefits with health information privacy concerns?** In: Flood CM (Editor), editor. *Data Data Everywhere. Access and Accountability?* Montreal, Que & Kingston, ON: McGill-Queen's University Press; 2011. p. 1-21.1.

(7) Willison DJ, Schwartz L, Abelson J, Charles C, Swinton M, Northrup D. **Alternatives to project-specific consent for access to personal information for health research: What is the opinion of the Canadian public?** *J Am Med Inform Assoc* 2007;**14:**706-12. Doi 10.1197/jamia.M2457

(8) Black C, McGrail K, Fooks C, Baranek P, Maslove L. Data Data Everywhere...: Improving access to population health and health services research data in Canada. Centre for Health Services and Policy Research 2005. Date accessed 07/08/2006. http://chspr.ubc.ca

(9) Commission on the Future of Health Care in Canada, Romanow RJ. Building on Values: The Future of Health Care in Canada Final report. Saskatoon: Commission on the Future of Health Care in Canada; 2002. www.hc-sc.gc.ca/english/care/romanow/index.html

(10) Lowrance WW. Privacy, confidentiality and health research. Cambridge: Cambridge University Press; 2012.

(11) Jamrozik K. **Research ethics paperwork: what is the plot we seem to have lost?** *BMJ* 2004;**329**:286-2867.

(12) *Implementation of the Data Protection Directive in Relation to Medical Research in Europe.* Aldershot: Ashgate Publishing Limited; 2004.

(13) *The Data Protection Directive and Medical Research Across Europe*. Aldershot: Ashgate Publishing Limited; 2004.

(14) Tri-Council Policy Statement : Ethical Conduct of Research Involving Humans - Second Edition, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada, (2012).

(15) Hebert P, Saginur R. **Research ethics review: Do it once and do it well.** *Canadian Medical Association Journal* 2009 Mar 17**;180**(6):597. Date accessed 08/11/2011. www.cmaj.ca/content/180/6/597.full.pdf+html

(16) Willison DJ, Emerson C, Szala-Meneok K, Gibson E, Weisbaum K, Fournier F. **Access to medical records for research purposes: Varying perceptions across Research Ethics Boards**. **Journal of Medical Ethics** 2008. Apr;34(4):308-14. doi: 10.1136/jme.2006.020032

(17) Willison D, Gibson E, McGrail K. **A Roadmap to Research Uses of Electronic Health Information.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston, ON: McGill-Queen's University Press; 2011.

(18) Kosseim P, General Counsel Office of the Privacy Commissioner of Canada. The Advent of Electronic Health Records (EHRs) in the Current Legal and Policy Context. Ottawa, Ontario; 2005. Date accessed 09/06/2006. www.privcom.gc.ca/speech/2005/sp-d_051130_pk_e.asp

(19) Mole D, Fox C. **Electronic data protection: Procedures need drastic improvement.** *British Medical Journal* 2005 May 3**;330**:537.

(20) Murray Long & Associates Inc., Digital Discretion Inc. Privacy Enhancing Tools and Practices for an Electronic Health Record (EHR) Environment: Phase 2 of a Research Report for Health Canada's Office of Health and the Information Highway. 2003.

(21) Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM, **Computerization of Medical Practices for the Enhancement of Therapeutic Effectiveness investigators. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data.** *BMJ* 2003 Feb 15;**326**(7385):373.

(22) Doyle P, Lane JI, Theeuwes JJM, Zayatz LV. **Introduction**. In: Doyle P, Lane JI, Theeuwes JJM, Zayatz LV, editors. *Confidentiality, Disclosure, and Data Access:*

*Theory and Practical Applications for Statistical Agencies*. Amsterdam: Elsevier Science B.V.; 2001. p. 1-15.

(23) Malhorta NK, Kim SS, Agarwal J. **Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model.** *Information Systems Research* 2004;**15(**4):336-55.

(24) Smith HJ, Milberg SJ, Burke SJ. **Information privacy: Measuring individuals' concerns about organizational practices.** *MIS Quarterly* 1996;**20**(2):167-96. www.jstor.org

(25) Willison DJ. **Trends in collection, use and disclosure of personal information in contemporary health research: Challenges for research governance.** *Health Law Review* 2005;**13**(2&3):107-13.

(26) EKOS Research Associates. Healthcare and the Internet: Part of the Rethinking the Information Highway Study. Health Canada; 2003.

(27) EKOS Research Associates. Understanding Privacy and Security: Part of the Rethinking the Information Highway Study. 2003.

(28) EKOS Research Associates Inc. Healthcare and the Internet: Part of the Rethinking the Information Highway Study. 2004.

(29) EKOS Research Associates Inc. Health Information and the Internet: Part of the Rethinking the Information Highway 2004/2005. 2005.

(30) EKOS Research Associates Inc. Electronic Health Information and Privacy: What Canadians Think-2007. 2007.

(31) EKOS Research Associates Inc. Wave 1 and Wave 2: Graphical Summary Report: Part of The Information Highway Study. 2007.

(32) Ipsos-Reid. Comfort in Access to and Disclosure of Personal Health Information. 2004.

(33) Ipsos Reid. The Canadian Medical Association: Canadian Views on Privacy. 2007.

(34) Canadian Institutes of Health Research. A Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research. Public Works and Government Services Canada; 2000. Report No.: MR21-22/2000E.

(35) EKOS Research Associates Inc. Public Attitudes to the EHRs and its Linkages. 2003.

(36) EKOS Research Associates. Pan-Canadian Health Information Privacy and Confidentiality Framework Study. 2004.

(37) EKOS Research Associates Inc. Canadians and the Privacy Landscape a Year Later. 2007.

(38) Kosseim P. Health research and data protection: How can researchers contribute to the policy debate? In: Flood CM (Editor), editor. Data data everywhere. Montreal, Que & Kingston, ON: McGill-Queen's University Press; 2011. p. 25-38.

(39) Lewis S. **Securing a Bright Health Information Future: Context, Culture, and Strategies.** In: Flood CM, editor. *Data Data Everywhere: Access and Accountability?* Montreal & Kingston: McGill-Queen's University Press; 2011. p. 253-66.

(40) Lysyk M. *A descriptive comparison of international and Canadian guidelines in health research privacy.* University of Ottawa, Ottawa, Ontario .(2013).

(41) Lysyk M. *What are Canadian university biomedical research ethics boards (REBs) requirements for protecting privacy? A descriptive review of REB policy and website guidance documents* . University of Ottawa , Ottawa, Ontario.(2013).

(42) Laufer RS, Wolfe M. **Privacy as a concept and a social issue: A multidimensional developmental theory.** *J Soc Issues* 1977;**33**(3):22-42.

(43) Luo X. T**rust production and privacy concerns on the internet: A framework based on relationship marketing and social exchange theory.** *Indust Marketing Management* 2002**;31(**2):111-8.

(44) Stewart KA, Segars AH. **An empirical examination of the concern for information privacy instrument.** *Information Systems Research* 2002;**13**(1):36-49.

(45) Culnan MJ, Bies RJ. **Consumer privacy online: Balancing economic and justice considerations.** *Journal of Social Issues* 2003;**59**(2):323-42.

(46) Milne GR, Gordon ME. **Direct mail privacy-efficiency trade-offs within implied social contract framework.** *Journal of Public Policy Marketing* 1993;**12**(2):206-15.

(47) Cohen RL. **Distributive justice: Theory and research**. *Soc Justice Res* 1987;**1**:19-40.

(48) Donaldson T, Dunfee TW. **Towards a unified conception of business ethics: Integrative social contracts.** *Acad Management Rev* 1994;**19**(2):252-84.

(49) Dunfee TW, Smith NC, Ross Jr. WT. **Social contracts and marketing ethics.** ***J Marketing*** 1999;**63(**July):14-32.

(50) Saxena N, MacKinnon M.P, Watling J, Willison D, Swinton M. Understand Canadian's Attitudes and Expectations: Canadians' Dialogue on Privacy and the Use

of Personal Information for Health Research in Canada. Canadian Policy Research Networks: Public Involvement Network; 2006. Report No.: Pl09.

(51) Lysyk M, Graham I, El Emam K. **A decade of public trust: Canadians' opinion on privacy and electronic health information.** *Electronic Healthcare***, submitted** 2013.

(52) Gerber E.R. **The privacy context of survey response: An ethnographic account. In: Doyle P., Lane J.I., Theeuwes J.J.M., Zayatz L.V**., editors. Confidentiality, Disclosure and Data Access: *Theory and Practical Applications for Statistical Agencies.* Amsterdam: ElsevierScience B.V.; 2001. p. 371-416.

(53) Canadian Institutes of Health Research. CIHR Best Practices for Protecting Privacy in Health Research. Ottawa: Public Works and Government Services Canada; 2005. Date accessed 20/05/2006. www.cihr-irsc.gc.ca/e/29072.html

(54) Health Canada. Pan-Canadian Health Information Privacy and Confidentiality Framework. 2005. www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php

(55) Weisbaum KM, Slaughter PM, Collins PK. **A voluntary privacy standard for health services and policy research: Legal, ethical and social policy issues in the Canadian context.** *Health Law Review* 2005**;1**:42-6. Date accessed 11/05/2011. www.law.ulberta.ca/centres/hlidev1/userfiles/7_Weisbaum-Slaughter-Collins.pdf

(56) Office of the Information and Privacy Commissioner of Alberta, News Release. Seven stolen or lost laptops in one month, no encryption Commissioner says "what the...". 2010. 15-12-2010. Date accessed 15/12/2010. www.oipc.ab.ca

(57) Office of the Privacy Commissioner of Canada, Address by Sandy Hounsell SRaOA. Health Information Privacy and Research. Remarks at the Atlantic Symposium on Privacy in Health Services and Policy Research, St, John's Newfoundland and Labrador.\ . 2009.
Ref Type: Internet Communication

(58) Health Council of Canada (January 2005). Health Care: Renewal in Canada: Accelerating Change. 2005. http://www.healthcouncilcanada.ca/rpt_det.php?id=170

(59) Assessing the Potential of National Strategies for Electronic Health Records for Population Health Monitoring and Research. Hyattsville, Maryland: U.S. Department of Health and Human Services, Centres for Disease Control and Prevention National Center for Health Statistics; 2006. Report No.: Series 2, Number 143.

## Appendix 1: Combined List of 162 Privacy Practices: Derived from CIHR BPPP and TCPS 2

**Note:**
**Green: Items related to creation of databases for general research purposes as classified by CIHR BPPP only; no classification of database items available in TCPS 2 (n=15)**
**Yellow: Items related to the secondary use of data as classified by both TCPS 2 and CIHR BPPP (n=12)**

| CIHR Principle# | Element Description | TCPS 2 Mapping |
|---|---|---|
| **Principle 1 (n=12)** | **Determining the research objectives and justifying the data needed to fulfill these objectives** | **Article 3.2; Article 5.3** |
| 1.1 | Identify and document the specific research objectives/hypothesis and related research questions | Article 3.2 (b) |
| 1.1.1 | Anticipate and document research questions related to the primary objectives that may become relevant after the initial data analysis | |
| 1.1.2 | Clear describe how data will be used, e.g., analysis, linkage, sharing) and how this relates to research question/ hypothesis | Article 3,2 (i); Article 5,3(b)(c)(g)(h) |
| 1.1.3 | Anticipate and document likely future uses of the data including possible collaborations or commercial uses | Article 3,2 (i)(e) |
| 1.2 | Creation of a database for general research purposes: | |
| 1.2.1 | • Define the scope and purpose of the database | |
| 1.2.2 | • Describe the types of studies that could be undertaken. | |
| 1.2.3 | • Describe what the database will not be used for. | |
| 1.2.4 | • Although future research purposes are not specified in detail, data management, storage and use will occur within a defined framework, including review and approval by an REB. | Article 3,2 (i); Article 5,3(b)(c)(g)(h) |
| 1.2.5 | • Describe the general types of personal data that are necessary for these general research objectives, e.g., diagnosis, risk factors, outcomes. Be as specific as possible. | 5.3 (a) |
| 1.2.6 | **Qualitative research**: anticipate and document all issues related to privacy and how privacy will be managed when employing inductive methodologies | Chapter 10(e); Article 10.1-3 |
| **Principle 2 (n=12)** | **Limiting the collection of personal data** | Article 3,2 ; Article 5,3 |
| 2.1. | Justify (statistically) and document sample size (participants/number of records required) for research question. | |
| 2.2. | Collection of sensitive data: Indicate if the data is considered sensitive, e.g., mental health, sexual attitudes, use of alcohol drugs, HIV status (see Table 2.1 for list): | Article 5.3 (d) |
| 2.2.1 | Specify privacy risk in terms of harm or stigma that might attach to the identification of an individual (for example, if the information were accidentally released) because of the nature of the information collected. Describe how privacy risk will be minimized and managed. | Article 5.3 (d) |
| 2.2.2 | Specify privacy risk (harm and stigma) that could be attached to the identification of a family or defined community because of the nature of the information, e.g., social or economic risks. Describe how privacy risks will be minimized and managed. | Ch 5: Key concepts<br><br>Article 5.3 (d) |

| | | |
|---|---|---|
| 2.3 | Justification for use of identifiable (vs. non-identifiable or aggregate) data for research question/ hypothesis: When directly collecting from individuals, justification can include a) need to contact individuals b) data linkage c) data accuracy check (coded data). **(includes Element 2.1.1 & 2.3.1)** | Ch 5: Types of Information ; 5.3 (a-h) |
| 2.3.1 | Identify and list each data element that will be collected: | Article 5,3:Application |
| 2.3.2 | Justify that each data elements that is a direct identifiers, e.g., name, street address, or that could potentially be used to identify an individual. (see Table 2.2) is needed to meet the research objectives. | |
| 2.3.3 | Justify that all data elements are at the minimal level of identifiability needed to meet the research objectives, e.g., use of age rangers vs. year of birth. | Ch 5: Types of Information |
| 2.3.4 | If identifiable data are required, when will these elements be removed? Describe the coding process that will be used, e.g., single, double/multiple. **(see Element 7.2.2.2)** | Ch 5: Types of Information |
| 2.3.5 | When sharing data, e.g., btw researchers: Demonstrate that the sharing of identifiable data has been minimized. | Article 5,7: Application |
| 2.4 | **Inductive data collection:** Protection of privacy<br>For inductive data collection, the extent of personal data to be collected may not always be foreseeable in detail at the outset of the interview. In these cases, demonstrate ongoing negotiation of consent with research participants to ensure that privacy of individuals and communities is appropriately protected. | Ch 10: (e); Article 10,2 |
| **Element 3 (n=17)** | **Determining whether consent from individuals is required** | Article 3.5;3.7 Article 5.5 |
| 3.1. | Collection from individuals: consent required when collecting PI directly from individuals (including by mail/email; meetings; telephone); involving procedures to screen for, prevent or treat dz, medical examination; clinical trials | Article 3.5 Article 5.5 |
| 3.1.1 | Collection from individuals: Researcher may request consent to be waived (part or all) with clear justification, e.g., min subject risk, waiver will not affect subject rights/welfare; consent not practical; when possible subject provided with additional pertinent information after participation; waived consent does not involve therapeutic intervention; consideration of jurisdictional legal requirements. | Article 3.7 (a-e) |
| 3.1.2 | Collection from individuals and data linkage: Consent should be sought for both activities (collecting data from individuals and data linkage) at the time of direct contact. | |
| 3.2 | Direct collection and secondary use (Hybrid model) – e.g., recruitment for secondary use | |
| 3.3 | Secondary Use (consent will be sought by researcher) | Article 5.5 |
| 3.3.1 | Secondary Use: Request for waiver of consent considerations | Article 5.5 |
| 3.3.1.1 | Necessity of the personal data (justification) | Article 5.5 (a) |
| 3.3.1.2 | Researcher outlines risk of harm (physical, psychological, social or economic risks including invasion of privacy or breach of confidentiality). REB determines minimal risk | Article 5.5 (b); Article 3.2 (c) |
| 3.3.1.3 | Research outlines benefits (REB determines benefits outweigh harm) | |
| 3.3.1.4 | Researcher justifies that obtaining consent is1) inappropriate or 2) impracticable (justification) | Article 5,5 (e) |
| 3.3.1.5 | Have individuals previously objected to this secondary use? If no or unknown, researcher with consider expectations of individuals | Article 5.5 (d) |
| 3.3.1.6 | Demonstrate consultation from well-defined groups or communities may, e.g., Aboriginals, family groups. | Article 5.5 Application |

| | | |
|---|---|---|
| 3.3.1.7 | Demonstrate jurisdictional legal requirements (federal/provincial/territorial) have been met. For example, some jurisdictions require some or all of the following:<br>- a data sharing agreement between the data holder and researcher<br>- notification and/or approval by other relevant oversight bodies<br>- agreement that personal data will not be used to contact individuals | Article 5.5 Application |
| 3.3.1.8 | Openness: Strategy for informing the public about the research | |
| NEW | REB review is not required for research using identifiable information:<br>a) the information is legally accessible to the public and appropriately protected by law; or b)the information is publicly available (there is no reasonable expectation of privacy) | Article 2.2 |
| NEW | REB review not required and for research that relies exclusively on secondary use of anonymous information, so long as the process of data linkage or recording or dissemination of results does not generate identifiable information | Article 2.4 |
| **Element 4 (n=8)** | **Managing and documenting consent** | Chapter 3 |
| 4.1.1 | Voluntary opt-in consent: subject can withdraw participation/identifiable data at any time without consequence **(see Element 5)** | Article 3.1 |
| 4.1.2 | I/A Presumed consent with opt-out (Note: researcher justifies why opt-in is deemed inappropriate or impracticable) | Article 3.1 |
| 4.2.1 | Document consent: Written documentation will be signed by the research participant (preferred) | Article 3.12 |
| 4.2.2 | Document oral consent, e.g., telephone interview: Researcher documents oral procedures | Article 3.12 |
| 4.2.3 | For highly sensitive information: Documented consent should not be linked to data or results of analysis | |
| 4.3 | **Qualitative data**: Researcher defines informed consent as ongoing negotiation, e.g., interview data. | Article 10.2-10.4 |
| 4.4. | Collecting information on individuals who do not wish to participate. Research must seek individual's consent or REB waiver | Article 10.3 |
| **Element 5 (n=45)** | **Informing prospective research participants about the research through informed consent** | Article 5.1-2<br>Article 3.2-3.12 |
| 5.1 | Information should be communicated in plain language in consent process | Article 3.2 (a-c) |
| 5.2 | Amount of time taken to communicate information should be appropriate to the need, and should be neither excessive nor too brief; sources of more study details should be provided | Article 3.2 (a-c) |
| 5.3.1 | Informing research participants about results related to themselves: During consent researcher determines a) whether participants wish to be informed of meaningful results b) how and through whom they should be communicated, e.g., genetic councilor or health-care provider. | Article 3.2 (f) |
| 5.3.2 | Informing populations (and government authorities) of general results and potential negative impacts | Article 3.2 (a-c) |
| 5.4 | **Qualitative research**: Consideration of participant/community involvement in writing and reporting process | |
| 5.5. | Providing information about privacy to prospective research participants **(see Elements 5.5.1- 5.7)** | Article 3.2 (i) |
| 5.5.1 | If appropriate: research participants receive copy of consent form | Article 3.12 |
| 5.5.2 | Research objectives and procedures to be included in consent form(general research) | Article 3.2. |
| 5.5.3 | Data types and uses, e.g., commercial, clinical care. | Article 3.2 (e) (i) |
| 5.5.4 | Voluntary basis for participation and ongoing opportunity to decide whether to continue | Article 3.2(d) |
| 5.5.4.1 | Voluntary basis for participation: withdraw without neg. effects during a study | Article 3.2 (d) |

| | | |
|---|---|---|
| 5.5.4.1.2 | Voluntary basis for participation: withdraw without neg. effects after a study is completed | Article 3.2 (d) |
| 5.5.4.2 | If withdraw (during or after), removal of identifying information from study (with exception of data that has been de-identified) | Article 3.2 (d) |
| 5.5.4.3 | Circumstances for researcher termination participants involvement | Article 3.2 (l) |
| 5.5.5.1 | Privacy risks are outlined, e.g., social or economic risks such as invasion of privacy or breach of confidentiality. | |
| 5.5.5.2 | Outline how privacy risks will be managed and minimized | |
| 5.5.6 | Research benefits and any compensation | Article 3.2 (j) |
| 5.5.7 | Clearly outline how confidentiality be maintained, e.g., according to relevant privacy/ATI legislation. | Article 3.2 (i); Article 5.1-2 |
| 5.5.7.1 | Identify and document external research partners confidentiality boundaries, e.g., Health Canada partner. | Article 3.2 (i); Article 5.1-2 |
| 5.5.8 | General description of security safeguards, e.g., coding of data, locked storage. | Article 3.2 (i); |
| 5.5.9 | Data access –who will have access to data (including researchers, REB, audit bodies, government ATI legislation) | Article 3.2 (i); Article 5.1-2 |
| 5.5.9.1 | Data access – will participants have access to data? Explain why not, e.g., data has been rendered de-identified. | |
| 5.5.9.2 | Legal disclosure requirements, e.g., public health, civil authorities. | Article 3.2 (i); Article 5.1-2 |
| 5.5.10 | To individual: when results will be reported back to individual or a clear statement if results will not be given | Article 3.2 (g) |
| 5.5.10.1 | To individual: when results will be reported back to individual thru their physician with counseling, e.g., genetic conditions. | Article 3.2 (g) |
| 5.5.10.2 | To family members: Conditions for informing family members must be clearly stated | |
| 5.5.11 | Data retention period | |
| 5.5.11.1 | Data retention period if extended/indefinite time-line for REB review | |
| 5.5.12 | Who to contact with inquires including withdrawal from study | Article 3.2 (h) |
| 5.5.12.1 | Who to contact regarding privacy, confidentially and security concerns or complains | |
| 5.5.12.2 | Who to contact with general questions, rights and complaints | Article 3.2 (h) |
| 5.6 | Collection from individuals and secondary use (Hybrid model) – inform participants of: | Article 3.2 (i) Article 5.5; 5.7 |
| 5.6.1 | All expected and types and sources of personal data to be accessed and used | Article 5.5 |
| 5.6.2 | All expected linkages | Article 5.7 |
| 5.6.3 | The expected purposes for which data will be used, e.g., health survey data to be collected and linked, with consent, to health records to investigate health-care use in the population. | Article 3.2 (i) |
| NEW | Additional requirements regarding research dealing with individuals who have lack capacity to consent | Article 3.9 (a-e) |
| NEW | Use of research directives to express participant's wishes on future uses of data collected and to guide researcher and authorized third party in the event that participant loses capacity to consent. | Article 3.11 |
| 5.7. 1 | Collection for database/ for multiple research purposes – inform participants of | |
| 5.7.1.1 | Expected studies that might be conducted, e.g., research on cardiovascular disease. | Article 3.2 (i) |
| 5.7.1.2 | Expected data typed and uses (linkage), for what research purpose | |
| 5.7.1.3 | What data will not be used for, e.g., studies outside of scope, linkage. | |
| 5.7.1.4 | Expected commercial uses | Article 3.2. (e) |
| 5.7.1.5 | Data retention period and if extended/indefinite time-line for REB review | |
| 5.7.1.6 | Process being implemented to endure proper stewardship and data security, e.g., advisory committee | |

| | | |
|---|---|---|
| **Element 6 (n=13)** | **Recruiting participants** | Article 3,1 |
| 6.1. | Include proposed recruitment procedure and materials in REB proposal. (Must foster conditions for voluntary consent; no coercion). | Article 3.1(a) |
| 6.1.2 | For all studies (including SU), indicate by whom and how eligible study subjects will be identified | Article 3.1(a) |
| 6.1.3 | Researcher requests to waive consent when assembling contact list of eligible individuals (REB decision). Note: legal restrictions | |
| 6.1.4 | Researcher/data custodian anticipates future recruitment uses of PI at the time of the original collection; appropriate consent obtained at that time | Article 3.1.2 |
| 6.2 | Initial contact and informing prospective participants | Article 3.1(a |
| 6.2.1 | Once identified, how will prospective research participants be recruited? | Article 3.1(a |
| 6.2.2 | Initial contact for recruitment is done by individuals that participants would expect to have relevant information about them, e.g., data holder. | |
| 6.2.3 | Trust vs. undue influence, e.g., if approached by data holder such as clinician, patient must be reassured that their reasonable expectation of care will be met regardless of decision to participate. | Article 3.1(a) |
| 6.2.4 | Documentation of any and all researcher conflict of interest (including those that may influence subject recruitment) **(see Element 1.1.4)** | |
| 6.2.5 | If researcher is given REB permission to contact subjects directly, prospective research participant has been made aware of diagnosis, e.g., cancer, that is used to determine eligibility | |
| 6.3 | REB application refers to preferred recruitment practices, e.g., institutional, CIHR. | Article 4.1 |
| 6.4 | Direct collection and secondary use (Hybrid model), e.g., recruitment for secondary use. All above apply; REB determines if consent is needed (included is Element 3.2) | |
| **Element 7 (n=28)** | **Safeguarding personal data** | Chapter 5 |
| 7.1 | Privacy safeguards should be proportional to privacy risks | Key concepts: Types of Information |
| 7.2 | Threat and risk vulnerability assessment on electronic systems has been conducted, e.g., networked computer systems housing electronic databases. | |
| 7.2. | Organizational safeguards-including: | Article 5.4 |
| 7.2.1. | • Institutions/organizations holding research data have appropriate institutions safeguards as demonstrated in policies and procedures. These should include: | Article 5.4 |
| 7.2.1.2 | • Appropriate privacy/security training **(see Element 8.1.3)** | |
| 7.2.1.3 | • All involved in the research project should be subject to a pledge of confidentiality **(see Element 10.2)** | |
| 7.2.1.4 | • Access to personal information should be strictly limited in terms of numbers of persons, for legitimate purposes, and strictly on a realistic need-to-know basis. **(see Element 8.1)** | Ch 5: Security |
| 7.2.1.5 | • Data-sharing agreements between the researcher/institution and all involved should be signed prior to providing any access to data. **(see Element 8.3)** | |
| 7.2.1.6 | • Consequences for breach of confidentiality, including dismissal and/or loss of institutional privileges, should be clearly stipulated. | |
| 7.2.1.7 | • Develop, monitor and enforce privacy and security policies and procedures; | Ch 5: Security |
| 7.2.1.8 | • Appoint privacy officers and create data stewardship committees as needed. | |
| 7.2.1.9 | • Implement internal and external privacy reviews and audits | |
| 7.2.2 | Technical measures including: | Ch 5: Security |

| | | |
|---|---|---|
| 7.2.2.1 | • Encryption, scrambling of data and other methods of reducing the identifiability of data should be used to eliminate unique profiles of potentially identifying information. | Article 5.3 |
| 7.2.2.2 | • Direct identifiers should be removed or destroyed at the earliest possible opportunity **(see Element 2.3.1)** | Ch 5-Types of Information |
| 7.2.2.3 | • If direct identifiers must be retained, they should be isolated on a separate dedicated server/network without external access. | |
| 7.2.2.4 | • Camouflage sampling or other techniques should be used, when appropriate, to prevent researchers from viewing health-related information of eligible individuals prior to gaining their consent. | |
| 7.2.2.5 | • Authentication measures (such as computer password protection, unique log-on identification, etc.) should be implemented to ensure only authorized personnel can access data. | Ch 5: Security; Article 5.3 |
| 7.2.2.6 | • Special protection for remote electronic access to data should be installed. | |
| 7.2.2.7 | • Virus-checking programs and disaster recovery safeguards such as regular back-ups should be implemented | Ch 5: Security; Article 5.3 |
| 7.2.2.8 | • Where possible, a detailed audit trail monitoring system should be instituted to document the person, time, and nature of data access, with flags for aberrant use and "abort" algorithms to end questionable or inappropriate access. | |
| 7.2.3 | Physical Security: | Ch 5: Security; Article 5.3 |
| 7.2.3.1 | • Computers and files that hold personal information should be housed in secure settings in rooms protected by such methods as combination lock doors or smart card door entry, with paper files stored in locked storage cabinets. | Ch 5: Security; Article 5.3 |
| 7.2.3.2 | • The number of locations in which personal information is stored should be minimized. | |
| 7.2.3.3 | • Architectural space should be designed to preclude public access to areas where sensitive data are held. | Ch 5: Security; Article 5.3 |
| 7.2.3.4 | • Routine surveillance should be conducted. | |
| 7.2.3.5 | • Physical security measures should be in place to protect data from hazards such as floods or fire. | |
| **Element 8 (n=9)** | **Controlling access and disclosure of personal data** | Chapter 5 |
| 8.1. | Access must be limited and on a need to know basis List who will have access to data (members of the research team, selected institutional employees, "deemed" employees or trusted third parties) | |
| 8.1.1 | Controlled access to personal data: Justify why these individuals must have access, e.g., roles/responsibilities. | |
| 8.1.2 | Required training and safeguards are in place for team members **(see Element 7** & Table 8.1) | |
| 8.2 | Justify need for data linkage related to research question/hypothesis | Article 5.7 (a) |
| 8.2.1 | Identify who will conduct data linkage and how. (see Table 8.1)<br>Preferred approach<br>(who) data holder : (how) data holder performs the linkage and removes all direct identifiers, or places direct identifiers with a code , prior to releasing the linked data set to the external researchers. (see Table 8.2) | Article 5.7 |
| 8.3 | Data sharing agreements that bind data providers and researchers to their respective responsibilities and obligations for protecting personal data (including coded data or where direct identifiers are removed) are in place before data sharing occurs outside research team. | |

| | | |
|---|---|---|
| 8.4 | Identify controls in place to minimize or avoid risks of inadvertent disclosures of individual's identities in public reports of research findings (See Statistics Canada guidelines available on-line) | Article 5.3 (c)<br>Ch 5: Types of Information<br>Article 5.1 |
| 8.4.1 | **Reporting qualitative research results** when concealing individual's identities is not desired. (In some qualitative studies, individual participants may understand and willingly accept the possibility that their identities may be revealed in the public reporting of research results) | |
| **Element 9 (n=8)** | **Setting reasonable limits on retention of personal data** | Article 5.3 |
| 9.1. | Specific research project: Justification of retention related to research objectives and as set-out in terms of original collection, data sharing agreements, institutional policies and legal requirements, e.g., such as university retention periods and regulations such as Food and Drug Regulations- Division 5-C.05.012 (4) records for clinical trials must be retained for 25 years. | |
| 9.1.1. | • Long-term retention of personal data should be subject to periodic audits and oversight by independent bodies including REBs | |
| 9.1.2 | Database for general health research purposes – may be retained for the general purposes originally consented to, subject to security safeguards proportionate to the identifiability, sensitivity and amount of the data, as well as its format and method. | |
| 9.1.2.1 | • Long-term retention of personal data should be subject to periodic audits and oversight by independent bodies including REBs | |
| 9.2 | Describe data storage, management and data access policies **(see Elements 7 &8)** | Article 5,3 |
| 9.2.1 | Describe how data (paper and electronic) will be disposed of or returned to the health information custodian (as set-out in terms of original collection, data sharing agreements, institutional policies and legal requirements) | Article 5,3 |
| 9.2.2 | Describe when data (paper and electronic) will be disposed of or returned to the health information custodian (as set-out in terms of original | Article 5.3 |
| **Element 10 (n=10)** | **Ensuring accountability and transparency in the management of personal data** | Article 2.1,<br>Article 5,2<br>Article 5.4 |
| 10.1 | Transparency (be open about research objectives; privacy policy practices). Consider relevant institutional/organizational privacy policies and procedures (**see Elements 3-5).** | Article 5.4 |
| 10.2 | Accountability: Researchers (principle investigator, researchers) **From signing responsibilities:** roles and responsibilities for PI, researcher team including pledge of confidentiality for all | |
| 10.2.1 | **From consent:**<br>-providing a mechanism to handle privacy queries and complaints<br>-promoting openness re purpose of research and privacy policies | |
| 10.2.1.2 | Academic and other affiliated hosting institutions include:<br>**From institution privacy policy:**<br>-designation of Privacy Officer; adequate training; mechanism for complains | |
| 10.2.1.3 | **From signing responsibilities/pledge of confidentiality**<br>-appropriate sanctions for non-compliance | Article 5.2<br>Article 5.4 |
| 10.3 | REBs (**Monitoring)**<br>Privacy related responsibilities include undertaking regular monitoring of research and coordinating reviews of multi-centre research to ensure equivalencies in standards across jurisdictions, by conducting: | Article 2.1 |

| | | |
|---|---|---|
| 10.3.1 | • an annual review of the research (required under TCPS); | Article 2.1 |
| 10.3.2 | • an audit of critical aspects of the research protocol including the consent process, safeguards and, where relevant, methods of reducing the identifiability of data prior to disclosure | Article 2.1 |
| 10.3.3 | • other effective monitoring mechanisms, as appropriate | Article 2.1 |
| 10.4 | Independent advisory/data stewardship committees **(includes Element 1.3)**<br>-Advisory committee for defining the scope and strategic priorities of the research. The responsibilities of this advisory committee could include: | |