



**Atlantic Symposium on Privacy in
Health Services and Policy Research**

**The Atlantic Regional
Training Centre**



**SYMPOSIUM
REPORT**

April 20-21, 2009

Sheraton Hotel Newfoundland
St. John's, NL



Report compiled and written by:
Amanda Hancock, B.Comm., Graduate Student ARTC, MUN Faculty of Medicine

Layout and design by:
Christa McGrath
Memorial University of Newfoundland

Symposium Academic Leads:
Dr. Vianne Timmons, President, University of Regina
Dr. Anne Kearney, Assistant Professor, School of Nursing & Faculty of Medicine,
Memorial University

Symposium Sponsors:
The ARTC acknowledges the Canadian Institutes of Health Research (CIHR; primary funder) and the Newfoundland and Labrador Centre for Health Information (NLCHI) for their symposium funding and support and the Canadian Health Services Research Foundation for their continued support.



Table of Contents

Section 1: Executive Summary	1
Section 2: Key Messages	2
Section 3: Legislative Landscape	4
Section 4: Key Themes	5
Theme 1 - Addressing Technological Complexities	5
Secondary Usage and Consent	5
Data Linkage and Accountability	5
Theme 2 - Demystifying Research	6
Public Perception	6
Existing Guidelines	6
Theme 3 - Creating and Maintaining Trust	6
Education and Awareness	7
Dealing with Breaches	7
Theme 4 - Finding Consistency through Collaboration	7
Shared Understanding	7
Centralizing Responsibility	8
Section 5: Concluding Remarks	9
Appendix A: Participating Organizations	
Appendix B: Summary of Proceedings	

Executive Summary

On April 20th and 21st, 2009, 72 participants from more than 30 organizations across Canada came together to talk about privacy in health services and policy research. The public and private sectors were represented, with participants hailing from various arms of federal and provincial governments. A vast amount of knowledge was brought to the table, as there were physicians, nurses, lawyers, researchers, students and privacy advocates in attendance, among others. This range of expertise and experience resulted in dynamic discussions that offered insight into the future requirements of privacy regulation in health care. The Symposium was funded by the Canadian Institutes of Health Research, the Newfoundland and Labrador Centre for Health Information and the Atlantic Regional Training Centre. The Symposium was organized by the Atlantic Regional Training Centre.

This document describes the legislative context in which the Symposium took place and provides an overview of four key themes - demystifying research, addressing technological complexities, creating and maintaining trust, and finding consistency through collaboration. These four key themes encompass the necessary next steps on privacy issues both provincially and nationally. It also provides a list of participating organizations (Appendix A) and an overview of the proceedings (Appendix B). Throughout the two-day Symposium, a variety of perspectives were voiced on many of the complex issues involved in privacy legislation: the unique issues within Atlantic Canada, the state of national and jurisdictional progress, and the experiences from countries around the world.

"Happiness lies, first of all, in health"

– Sandy Hounsell quoting George William Curtis

[1842-1892 in Opening Address]

Key Messages

Discussions in the plenary and breakout sessions confirmed that participants unanimously agreed that trust is the foundation of all health care systems and the research that supports them. Trust is a privileged aspect of patient-provider relationships and is ingrained in the fiduciary duties of all health care professionals. It is essential that all users and providers of health care feel confident about the security and protection of patient information. Raising awareness amongst health systems users and professionals alike about the measures that are in place to keep data secure is one of many important tasks left to accomplish.

A second common sentiment was that there is still much work to be done to achieve balance between protection and permission. This referred specifically to the competing interests of protecting personal health information to respect individual rights to privacy, and allowing data custodians and researchers to access personal health information for beneficial purposes, such as research. Part of achieving the balance will require informing and educating all stakeholders, especially politicians and the public, about the nature and purpose of health services research.

“There are fundamental tensions between access and privacy.”

- Don Willison, Ontario Agency for Health Protection and Promotion

Canadian stakeholders are now in a strong position to draw from demonstrated best practices to create shared understanding as they work collaboratively towards an integrated system of Electronic Health Records (EHR). The two-day forum revealed four key messages about the current realities and future requirements of privacy in health care and health services research, which are summarized here and explained in detail throughout the body of the document:

1. **Addressing Technological Complexities** - The rapid pace of technological change is a main driver of the need to make progress in provincial and national privacy regulation. Technological breakthroughs that have made the possibility of achieving a nationally integrated system of Electronic Health Records (EHRs) a reality have also increased vulnerability by offering easy access to extensive amounts of sensitive information. Participants continually reiterated the need for clearer guidelines concerning contentious technology issues such as secondary/allowable usage, data linkage, consent, transparency and accountability.
2. **Demystifying Research** - Given the importance of and reliance on public opinion to support decision-making and agenda-setting, it is necessary to raise awareness about research through education. Participants were of the opinion that, in general, Canadians support research when they understand its benefits and feel confident that their health information is in safe hands. It is necessary to make the difference between collecting information for population health surveillance, scientific research, and commercial research widely known.

3. **Creating and Maintaining Trust** - As the method of storing personal health information changes to something new and unfamiliar with a seemingly large potential for breaches, it is necessary to build and maintain the public's trust. This will serve a dual role to further research capacity and increase overall efficiency of health care.
4. **Finding Consistency Through Collaboration** - Inconsistent laws and language were seen as an impediment to progress. Canadian researchers, health care providers, and data custodians of any kind have a common interest in maintaining public trust. As such, there is great potential for synergistic efforts around health information legislation and enhancing protection of personal information. This is particularly apparent in the Atlantic Provinces where all four provinces face similar issues.

Legislative Landscape

It is necessary to understand the nature of Canada's health care and justice systems to understand the context in which these four themes were identified. The majority of Canadian health care services are supported by public federal funds and delivered through provincially regulated systems. There are, however, certain aspects of this publicly funded sector that are delivered through private functions. As such, health care is both a public- and private-sector activity. Private health care delivery refers to those services provided in the course of commercial activity; this includes but is not limited to physicians in private clinics, laboratory services and pharmaceutical sales.

Privacy laws vary between sector and provincial and territorial jurisdiction. Specifically, the Privacy Act applies to the federal public sector, while the Personal Information Protection Electronic Documents Act (PIPEDA) applies to the federal private sector. The Privacy Act is widely criticized for being outdated and underprepared to deal with change, particularly technological advances. If provincial legislation has been developed and deemed an adequate equivalent, it can override PIPEDA in that region. PIPEDA has been replaced by provincial legislation in British Columbia, Alberta, Quebec, and Ontario.

Each of the Atlantic Canadian provinces is at a different stage of development in creating private-sector legislation to replace or supplement PIPEDA. In Newfoundland and Labrador, certain geographical and historical considerations have made the region ideal for key areas of research, such as genetics. As such, NL has recently passed the Personal Health Information Act through the House of Assembly. Provincial representatives from the Newfoundland and Labrador Centre for Health Information (NLCHI) as well as the Office of the Information and Privacy Commissioner expressed their hopes for proclamation of this Act in the near future. On the other hand, PEI remains in the early stages of talking about developing province-specific health information legislation.

Given these systemic complexities, knowledge of the applicable laws varies between disciplines of health care providers and the general public. Participants stressed the importance of creating awareness and understanding of the direct and practical implications of newly passed legislation to health care professionals' everyday working environments, particularly for those handling patient information.

Key Themes

Theme 1 - Addressing Technological Complexities

Canada Health Infoway is an independent, federally funded, not-for-profit organization that is accelerating the development of electronic health records across Canada. While participants saw the value of this integrated system, there was grave concern that it will provide data custodians with unlimited access at the click of a button. In a breakout session, one participant gave an example of an HIV-positive patient living in a rural area who did not want the local pharmacist to have access to his health record. Participants continually reiterated the need for clearer guidelines over several contentious issues, including secondary usage, consent, data linkage, transparency and accountability.

Secondary Usage and Consent

Participants expressed concerns that the current EHR protocol lacks any references to secondary usage. Secondary usage refers to the premise that data given to a researcher or group of researchers may be subsequently shared with other researchers and decision-makers. The main concern with secondary usage is the possibility of broad, open-ended consent that would provide researchers and decision-makers with unrestricted usage of individual patient information for a variety of purposes for an indefinite amount of time. The alternative method would be to return to patients or participants repeatedly and request consent every time their information is used. An anecdote of genetic research was provided to illustrate that study participants felt confused when the researchers continually returned for consent. The story demonstrated how a sense of distrust can be created when people are asked to provide consent on multiple occasions after having already agreed to release their personal information at the first instance. This introduces the possibility of consent fatigue. When consent fatigue occurs the spirit of what consent is all about in the first place - information and clarity - can be lost. This issue is an ongoing struggle for research ethics boards across the country and, as such, merits attention.

Data Linkage and Accountability

Data linkage refers to adjoining datasets to obtain more complete information. While this is desirable from an information standpoint, the ease of access creates a requirement to regulate data linkage and educate data custodians of limitations. The question "Who owns the data?" came up when discussing the various formats in which personal health information is stored - electronic health records, electronic medical records and personal health records. The view that the person whose information is contained in a particular file is the owner of the data was expressed. This right of ownership holds true through each additional layer of data linkage. As the discussion progressed, however, it became clear that while the patient is and will always be the ultimate data owner, the stewardship responsibilities fall on health care providers, researchers, and any other data custodian. Stewardship requirements see that someone is accountable for how and when records are accessed and the way in which the personal health information can be used.

Theme 2 - Demystifying Research

After reaching consensus that it is necessary to educate the public about research as a matter of priority, participants discussed which aspects of research require clarification. It is necessary to clarify the difference between collecting information for the purposes of population health surveillance, scientific research, and commercial research. Similarly, it would be beneficial to communicate recent research trends, including the ongoing shift towards studies that examine patient safety of medical techniques or devices that are new to the market. Such studies could diminish the occurrence of adverse events with new or understudied drug treatment regimens and devices. Many participants suspected that Canadians support research when they understand its benefits and feel confident that their personal health information is in safe hands. Researchers stressed that in the vast majority of studies, the identity of the person whose information is being used is largely immaterial to the findings. Oftentimes, the data is "de-identified", meaning all positive patient identifiers are removed from the dataset.

Public Perception

Due to the widespread usage of patient-centred care models, public opinion is a valued indicator of all aspects of health care – specifically, quality, delivery, privacy, and research. Throughout the Symposium, many facts and public opinion polls were cited to support claims made or actions taken by an individual or an organization. Due to Canada's massive geography and diverse population, participants stressed the importance of identifying the demographics of the samples used to measure public opinion. This is particularly important in the Canadian legislative context since privacy is regulated by jurisdiction and the result of a public opinion poll in central or western regions of the country may not be applicable to the Atlantic Provinces.

Existing Guidelines

In the provinces where PIPEDA has not been enhanced by provincial legislation, the Tri-Council Policy Statement is the only document that sets guidelines for protecting privacy in research. This document was created in 1998 (with amendments in 2000, 2002, and 2005) by national health research organizations. It is the most formal measure of protection of health information during research, yet it is widely recognized as an "ethics-based" document that contains vague information provisions and lacks enforceability. This leads to a variety of challenges related to project or study-specific interpretations, particularly where the research areas are a matter of national priority such as Aboriginal communities. It suggests best practices but lacks formal punitive measures that are applied in the event of an unethical occurrence, such as a privacy breach. Ultimately, this uncertainty can foster distrust; an updated and comprehensive version of this document could help create and maintain public trust.

Theme 3 - Creating and Maintaining Trust

Given the changing nature of data storage and access, privacy must remain a visible priority on political and organizational agendas. In the event of recent breaches, specific and methodical steps must be taken to restore, maintain, and build public trust. Achieving this will improve researchers' capacity to obtain useful information and increase the overall quality and efficiency of our health care systems. In addition to an updated Tri-Council Policy Statement for health

research involving humans, other suggestions included creating shared understanding of key terms, developing appropriate legislation, implementing adequate security measures, demonstrating organizational compliance, and ensuring that all storage of access to personal health record is for non-malicious purposes.

Education and Awareness

Participants felt that education of all stakeholders, including patients, health professionals and data custodians from all disciplines, is necessary. Importance was placed on the need to educate politicians on relevant issues so the priority and sensitivity of these issues is reflected in the proper decision-making arenas. Currently, there are varying levels of knowledge about current privacy regulations between disciplines. All data custodians must be educated and held to standards of trust to ensure both that appropriate data management techniques are in place and that they themselves trust in the system. This requires informing health care providers about the controls that are in place to protect individual data under increasingly automated systems. It is necessary to instill a sense of security about data storage and access in health care workers before it can be achieved in the public at large.

Dealing with Breaches

Although researchers stress that in the vast majority of scientific studies, information is de-identified and identities are largely immaterial, the reality must be addressed that there have been cases where personal information has been wrongly exposed. If trust is lost through breaches or other demonstrated misuse, people will be less likely to share their personal health information. Health care workers, researchers, and data custodians who deal with sensitive, personal information on a regular basis must be reminded of its sensitive nature from time to time. Such cases are particularly damaging because health care providers and relationships function within a small community in which trust is an integral component. Given public knowledge of such events, it is now necessary to raise awareness about what is being done to protect personal health information in the various jurisdictions. Under the EHR system, Canada Health Infoway must provide specific descriptions of how this will be accomplished.

“Trust is the bedrock of how and why we practice medicine.”

- Gerard Farrell

Theme 4 - Finding Consistency through Collaboration

It is necessary to continue discussing challenging issues and working towards developing solutions that were developed at the Symposium. Balance will not be achieved until there are mutually satisfactory ways to support health research while controlling privacy by developing answers for challenging privacy issues.

Shared Understanding

It is necessary to have a common understanding within the community to talk about and create policies that will allow for pan-Canadian work. This requires formalizing definitions for terms and

concepts that will satisfy all the intended uses of EHR, including patient care, health services and policy, as well as administrative uses. A preliminary list of terms and concepts for clarification is as follows:

Pertaining to Data Storage	Concepts
De-identified Coded Information Anonymous Use Disclosure Share	Secondary Usage Consent – informed, implied Circle of care Governance

Centralizing Responsibility

It is necessary for a national body to take responsibility for promoting strong and consistent privacy measures in health care systems across Canada. Due to the diverse backgrounds of participants, there was a wide range of degrees of understanding about the role of Canada Health Infoway and the progress that has been made on the implementation of EHR. Given this lack of understanding, participants suggested that a description of the project activity and progress at the beginning of the Symposium, as well as a statement of all benefits related to having an EHR system, would have provided a frame of reference for discussing the issues. Similarly, participants saw significant value in Newfoundland and Labrador's Centre for Health Information and felt it would be beneficial to have one in each province. The Centre had a key role in advancing the recently passed Personal Health Information Act and was described as a provincial centre of excellence that works with all stakeholders to further progress on legislative issues and to develop evidence-informed solutions.

Concluding Remarks

An individual's personal health information will always belong to the patient from whom it was obtained. In the move towards an electronic system of health records, the responsibility for handling and protecting this personal health information will be increasingly bestowed on others - health care professionals, researchers, and data custodians of any kind. The potential benefits from increased efficiencies in the resource scarce field of health care should not be underestimated. In the long run, the ability to obtain accurate and timely information will save time, money, and lives. While the idea of a person's entire medical history becoming available at the click of a button seems daunting, there are measures that can be taken to secure the information and reduce public uncertainty.

Data custodians must be provided with clear and operable standards for data management - from terminology to techniques - so that personal health information can be used effectively to further scientific advancement in a way that respects patients' right to privacy. Health care professionals must trust the quality of electronic systems and privacy controls in order to create a similar confidence in patients. Key players in both public and private sectors must ensure that privacy issues become a higher-priority item on organizational agendas. Policy-makers and legislators must work collaboratively to create language and develop guidelines that can serve the dual role of addressing challenging regional issues while providing a degree of inter-provincial consistency. Individual researchers and federal health care bodies must work to raise awareness about privacy issues by educating the public and key stakeholders on the benefits of research and the purpose and progress of Canada's EHR.

APPENDIX A

Participating Organizations

Atlantic Regional Training Centre	Nova Scotia Health Research Foundation
Canadian Institute of Health Information	Office of the Information and Privacy Commissioner for Newfoundland and Labrador
Captain William Jackman Memorial Hospital	Office of the Information and Privacy Commissioner, Prince Edward Island
Dalhousie University Dalhousie Health Law Institute Office of Research Ethics Administration	Office of the Ombudsman, New Brunswick
Department of Health and Community Services, NL	Office of the Privacy Commissioner of Canada
Department of Health, NB	Ontario Agency for Health Protection and Promotion
Department of Health, NS	Pictou County Health Authority
Department of Health, PEI	Regional Health Authority B, New Brunswick
Facilicorp, NB	The Nova Scotia Freedom of Information and Protection of Privacy Review Office
IWK Health Centre	University of New Brunswick Department of Computer Science and Applied Statistics Faculty of Law
McInnes Cooper	University of Prince Edward Island
Memorial University of Newfoundland and Labrador Community Health and Humanities Faculty of Medicine - Primary Healthcare Research Unit eHealth Research Unit Office of Research and Graduate Studies School of Nursing	Funders Canadian Institutes of Health Research (Primary Funder) Newfoundland and Labrador Centre for Health Information Atlantic Regional Training Centre
Ministry of Health, PEI	
National Research Council	
New Brunswick Health Council	
Newfoundland and Labrador Centre for Applied Health Research	
Newfoundland and Labrador, Central Regional Health Authority	
Newfoundland and Labrador, Eastern Regional Health Authority	
Newfoundland and Labrador, Western Regional Health Authority	
Newfoundland and Labrador Centre for Health Information	
Nova Scotia Freedom of Information and Protection of Privacy Review Office	

APPENDIX B
Summary of Proceedings

Agenda
Atlantic Symposium on Privacy in Health Services and Policy Research

Day 1: Monday, April 20

7:30 – 8:45 am	Registration and Breakfast
8:45 – 9:15 am	Welcome and Greetings
9:15 – 10:00 am	Opening Address
10:00 – 10:15 am	Refreshment Break
10:15 – 11:30 am	Public Goods and Private Rights: The Use of Personal Health Information for Research Purposes
11:30 – 12:30 pm	EHRs: Current Debates and Future Considerations
12:30 – 1:30 pm	Lunch
1:30 – 2:30 pm	Concurrent Session 1: 1A: The Benefits of the Secondary Use of EHR/Administrative Data 1B: Managing Privacy Breaches 1C: Current Issues with Managing Access Requests
2:30 – 3:00 pm	Refreshment Break
3:00 – 4:00 pm	Concurrent Session 2: 2A: Privacy Breaches—A Perspective from the NL Commissioner’s Office 2B: The Interaction Between Health Research and Policy: Can They Co-Exist? 2C: Health Information Protection Legislation
4:00 – 4:30 pm	Day 1 Wrap Up
7:00 – 9:00 pm	Café Scientific Why Do You Want to Know That? The Use of Personal Health Information in Health Services and Policy Research

Day 2: Tuesday, April 21

7:30 – 9:00 am	Networking and Breakfast
9:00 – 10:30 am	Breakout Session
10:30 – 11:00 am	Refreshment Break
11:00 – 12:00 pm	Large Group Report Back and Wrap-up
12:00 – 1:00 pm	Lunch