Privacy and EHR Information Flows in Canada

Common understandings of the Pan-Canadian Health Information Privacy Group

Canada Health Infoway
Inforoute Santé du Canada

Pan-Canadian
Health Information
Privacy Group

June 30, 2010

Acknowlegements

This document is the result of the dedicated efforts of the members of the Health Information Privacy (HIP) Group, the support of Canada Health Infoway and the contributions of subject matter experts whose presentations, research, feedback and other input have enriched this paper. A list of HIP Group members is included in Appendix D.

Table of Contents

Appendices

Appendix A: Summary list of Common Understandings

Appendix B: Examples of Jurisdictional EHR Governance Models

Appendix C: Potential Options for the Structure and Roles of a
Pan-Canadian Body for Privacy and Related Information Governance

Appendix D: List of HIP Group Members, 2008-2010

Appendix E: List of presentations

Background Papers

MacPherson, Don and Ross Fraser, Jurisdictional Scan of Patient Notices, November 2008
http://www2.infoway-inforoute.ca/Documents/Jurisdictional_Scan_of_Patient_Notices_EN_FINAL.pdf

Fraser, Ross and Don Willison, Tools for De-Identification of Personal Health Information, September 2009
http://www2.infoway-inforoute.ca/Documents/Tools_for_De-identification_EN_FINAL.pdf

El Emam, Khaled, Practices for the Review of Data Requests and the Disclosure of Health Information by Health Ministries and Large Data Custodians, June 2010
http://www2.infoway-inforoute.ca/Documents/Practices_for_the_review_of_data_requests_June_2010_EN_FINAL.pdf

Sawatsky, Elaine, Information Sharing Agreements for Disclosure of EHR Data within Canada, January 2010
http://www2.infoway-inforoute.ca/Documents/ISA_report_for_HIP_Group_January_2010_EN_Final.pdf

Other References

White Paper on Information Governance of the Interoperable Electronic Health Record:
http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf

Conceptual Privacy Impact Assessment of Canada's
Electronic Health Record Solution Blueprint Version 2:
http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf

CSA Model Code for the Protection of Personal Information:
http://www.csa.ca/cm?c=Page&childpagename=CSA%2FLayout&cid=1239124810319&pagename=CSA%2FRenderPage

Pan-Canadian Health Information Privacy and Confidentiality Framework:
http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php

Executive Summary

Health information is currently disclosed from a trustee or custodian in one jurisdiction to a trustee or custodian in another jurisdiction in Canada for care and treatment and for secondary uses. It is important to jurisdictions that such trans-jurisdictional disclosures and collections continue to be supported in the new interoperable electronic health record (iEHR) environment in a privacy-protective manner.

The White Paper on Information Governance of the Interoperable Electronic Health Record and the Conceptual Privacy Impact Assessment of Canada's Electronic Health Record Solution Blueprint Version 2 identified privacy-related information governance issues that were non-technical in nature but were needed to support the flow of EHR information from one jurisdiction to another. At its 2007 Annual General Meeting, Canada Health Infoway's members (the Deputy Ministers of Health of Canada's fourteen jurisdictions) asked for assistance in addressing these common issues.

As a result, the Pan-Canadian Privacy Forum on EHR Information Governance was established in November, 2007, to share information and approaches. The Privacy Forum is comprised of one representative from the office of each jurisdiction's Privacy Commissioner or Ombudsman and one from each Ministry of Health across Canada.

Subsequently, the Pan-Canadian Health Information Privacy (HIP) Group was formed in December 2008, composed of the Ministry representatives of the Privacy Forum, to further the work and thinking on these issues.

As its first contribution, the HIP Group has put forward 33 'common understandings' to support appropriate and privacy protective trans-jurisdictional disclosures of EHR information for care and treatment and for secondary uses. The common understandings represent principles that the HIP Group believes should be adopted consistently across jurisdictions.

The common understandings reflect the general consensus of the HIP Group members in that most members generally agreed with the statements. Those members not in complete agreement with a particular common understanding (sometimes because of their jurisdiction's legislative environment) did not actively oppose it. Quebec participated in and contributed to the HIP Group: however, the differences in its legislative framework and EHR approach precluded it from being able to support all of the common understandings.

There is no intention to bind jurisdictions; rather, the paper emphasizes jurisdictional responsibility for decisions in these areas. The common understandings can, however, be valuable in promoting consistency and informing jurisdiction work on health information privacy legislation, associated health information or ehealth policies, information sharing agreements and business/technical requirements for EHR systems.

The 33 common understandings (the full list can be found in Appendix A) encompass:

- **Foundational understandings**: which set the stage for appropriate, privacy protective trans-jurisdictional disclosures of personal health information in a multi-jurisdictional EHR context.
- **Understandings related to trans-jurisdictional disclosure and collection of EHR information within Canada**: which set out some basic principles for EHR information flows across jurisdictions (e.g., once information has been disclosed to another jurisdiction the information becomes subject to the receiving jurisdiction's data protection laws.)
- **Understandings related to patient control of their personal health information in the EHR and patient notices about EHRs**: which set out principles for handling information that patients have chosen to 'mask', as well as some key messages for patient notification tools.
- **Understandings related to trans-jurisdictional disclosures of EHR information for secondary uses**: which address topics such as the use of de-identified information; the need for privacy risk assessments; patient information about trans-jurisdictional disclosures for secondary uses; and governance of trans-jurisdictional disclosures for secondary use.
- **Understandings related to accountability for information governance of the iEHR**: which speak to the importance of jurisdictional EHR governance structures including a privacy and information governance component and being accountable to a Minister.

The final two common understandings relate to the need for a *single integrated pan-Canadian group* to discuss, address and coordinate common privacy related information governance issues. The current HIP Group includes the core representation and activities of such a structure, but there is a need for discussion about the potential evolution of the HIP Group's mandate and composition. A range of alternatives is provided for consideration.

Introduction and Background

Jurisdictions are at various points in developing and implementing the information systems that make up their EHR network. They must manage their internal EHR priorities and expectations within budget and other resource restraints and are also working to ensure that appropriate supporting legislation and/or policies are in place. These are massive undertakings requiring an internal, jurisdictional focus.

The vision of the interoperable EHR (iEHR), however, involves information being available where and when a patient is treated or follow-up care provided. While most health care activity occurs within a patient's home jurisdiction, patient care can take place in a jurisdiction other than the patient's home jurisdiction. Examples include emergency care, some specialized care, specific services such as the reading of diagnostic images, and regular care for residents of many rural, remote, northern and border communities. Patient information is currently disclosed by a trustee or custodian in one jurisdiction and collected by a trustee or custodian in another for these purposes.

Health information is also used for many purposes other than care and treatment, such as managing the health system, processing claims, improving health care and patient safety, expanding knowledge about illness and disease, strengthening the effectiveness and efficiency of health care delivery, and supporting public health initiatives. Information currently flows within jurisdictions and in some cases to other jurisdictions for these purposes as well.

It is important to jurisdictions that all of the above trans-jurisdictional disclosures and collections continue to be supported in the new EHR environment and that they be accomplished in a coordinated and privacy-protective manner.

As work on the iEHR has progressed, a number of privacy related information governance issues[1] have been identified, notably in the following:

- The 2007 *White Paper on Information Governance of the Interoperable Electronic Health Record* identified a number of issues around trust and accountability, the privacy rights of patients and other topics for policy makers to consider in developing policies and related non-technical measures to support the interoperability of the iEHR.
- The 2008 *Conceptual Privacy Impact Assessment of Canada's Electronic Health Record Solution Blueprint Version 2* concluded that the Blueprint strongly supported patient privacy and that properly implemented, EHR Infostructure initiatives underway presented an unprecedented opportunity to bolster privacy. The report also made observations on policy-related information governance issues.

[1] *The term "information governance" in this paper refers to the rules, requirements and mechanisms involved in managing personal health information in the EHR as it relates to privacy, although there may be some overlap with other areas, e.g., data governance, system governance and corporate governance.*

At *Infoway's* 2007 Annual General Meeting, its members (the Deputy Ministers of Health of Canada's fourteen jurisdictions) recognizing that work needed to get underway on trans-jurisdictional issues in preparation for the future, asked for assistance in addressing the issues that had been raised. As a result, the Pan-Canadian Privacy Forum on EHR Information Governance was established in November, 2007, to share information and approaches.[2] Subsequently, the Pan-Canadian Health Information Privacy (HIP) Group, composed of the Ministry representatives of the Privacy Forum, was established in December 2008 to further the work and thinking on these issues and to share that knowledge.

As its first contribution, the HIP group has developed a series of common understandings on a number of topics related to the trans-jurisdictional disclosure of information from the EHR. These understandings, which are set out in this paper, are a mix of high level and more prescriptive principles that the HIP Group believes should be adopted consistently across jurisdictions to support trans-jurisdictional disclosures of personal information in a manner that is respectful of privacy and the differing approaches adopted by the jurisdictions. It is important to note that:

- The common understandings were considered within the context of current jurisdictional legislation, the principles of the Canadian Standards Association *Model Code for the Protection of Personal Information* and the *Pan-Canadian Personal Health Information Privacy and Confidentiality Framework*.[3]
- The common understandings reflect the general consensus of the HIP Group members. For the purpose of this work, this means that most members generally agreed with the statements and that those members not in complete agreement with a particular common understanding (sometimes because of their legislative environment) did not actively oppose it. Quebec participated in and contributed to the HIP Group: however, the differences in its legislative framework and EHR approach precluded it from being able to support all of the common understandings.
- Although the focus is on trans-jurisdictional disclosures of EHR information within Canada, some of the common understandings speak to the jurisdictional level. In part this is because jurisdictions recognize the desirability of consistent practices at the jurisdictional level, and in part, it is because trust in each other's information handling practices is required for jurisdictions to be comfortable making trans-jurisdictional disclosures.
- The HIP Group recognizes that EHR privacy issues go hand-in-hand with security and technology issues, and that several of the common understandings have technical and security implications. This paper, however, is focused on the privacy aspects of trans-jurisdictional disclosures.

[2] *The Privacy Forum includes representatives from each federal/provincial/territorial Ministry of Health and Privacy Oversight body. It provides a collegial setting for jurisdictions to share knowledge and experiences, and leverage their collective wisdom to facilitate the development of common solutions that can be considered by jurisdictions when making policy choices.*

[3] *The Framework was created for the Advisory Committee on Information and Emerging Technologies and endorsed by the Federal/Provincial/Territorial Conference of Deputy Ministers of Health. Saskatchewan and Quebec did not endorse the framework document. The Framework can be found at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php*

- There is no intention to bind jurisdictions. The authors of this paper understand fully that jurisdictions are responsible for the laws, policies and systems developed and implemented within their boundaries and that within their laws, jurisdictions will determine how to interface with another jurisdiction. The common understandings are meant only to facilitate inter-jurisdictional thinking on these topics and promote consistency in approach, thereby facilitating the controlled and appropriate disclosure of personal health information across jurisdictions in authorized circumstances. The participation of ministry officials in the development of the common understandings is in no way to be interpreted as binding the jurisdictions to these positions.
- The paper does not address every information governance issue that has been raised, or every aspect of an issue.

An earlier draft of this paper was shared for informal comment by HIP Group members internally within their jurisdictions, internally within Canada Health Infoway and the Canadian Institute for Health Information, and with the pan-Canadian Privacy Forum.

Purpose and structure of this paper

This paper is meant to serve as a vehicle for sharing and discussing with other stakeholders (e.g., clinicians, policy makers, system designers) the HIP Group's common understandings. It is structured as follows:

Section 1
focuses on trans-jurisdictional disclosures of personal health information from the EHR within Canada, as well as patient control of their personal health information in the EHR and patient notices about EHRs

Section 2
focuses specifically on trans-jurisdictional disclosures of EHR information for secondary uses

Section 3
looks at accountability for information governance of the iEHR.

Notes on Terminology

Different jurisdictions use different terms for EHR-related activities in legislation and in the field. Some of these terms, such as 'custodian' and 'trustee', are defined in a jurisdiction's legislation. Other commonly-used terms are not set out in legislation but are descriptive – such as 'information flows', 'sharing' and 'viewing'.

Jurisdictions will of course continue to use terms as defined in their own legislation and practice. However, the HIP Group has agreed to use common definitions for certain terms in order to facilitate their discussions and they are used throughout the paper as described below.

- **Disclosure and indirect collection:** Information that 'flows' from, is 'shared' by or 'made available' by a custodian or trustee in one jurisdiction for 'viewing' by an authorized health care provider or organization in another jurisdiction constitutes a disclosure of that information by the first jurisdiction and an indirect collection by the second jurisdiction.[4]
- **Access:** 'Access' is often defined in jurisdictional legislation to refer to a person's ability to view or receive copies of their own information. The term can also refer to activities under various access to information/freedom of information statutes. In other contexts, including the iEHR context, it often refers to any action that involves an authorized individual being able to view, use, or modify a record. If the term 'access' is used with no qualifier, it refers to the third sense of the word. The paper uses qualifiers, e.g., "patient access to his or her information", or "access under access to information legislation" to refer to the other senses of the term.
- **Masking:** Jurisdictions use various terms – e.g., 'consent directives', 'disclosure directives', 'expressed wishes' – in legislation or policy, to describe how a patient can exercise a measure of control to restrict access to, use and/or disclosure of his or her personal information. Masking is the function used to operationalize this principle of patient control.[5] (Note: while recognizing that Ontario uses the term 'lock' or 'lock box' to describe this activity, the HIP group agreed to use the term 'masking' in its discussions.)
- **Secondary use:** While the HIP Group recognizes that there is ongoing debate about the division between primary and secondary use, in this paper, secondary use refers to the utilization of health information for any purpose other than the provision of direct care and treatment.
- **Accountability:** This refers to responsibility for decisions related to the collection, access, use, disclosure, retention and overall protection of personal health information. It encompasses accountability to the patient for the protection of his or her personal health information; as well as accountability to a Minister or other body for the good management of information in the iEHR.

[4] *Note that all transactions within Alberta Netcare are "uses", not disclosures*

[5] *Note that this relates to control over the INFORMATION in the record, not consent for treatment.*

Section 1:

Pan-Canadian common understandings to support trans-jurisdictional disclosures of EHR information within Canada

Section 1:
Pan-Canadian common understandings to support trans-jurisdictional disclosures of EHR information within Canada

All jurisdictions in Canada have a variety of statutes in place that enable and govern the collection, use and disclosure of personal health information for care and treatment and for secondary uses. Many jurisdictions are also putting in place supporting legislation and/or policies to reflect the new EHR context.

As noted in a paper prepared for an *Infoway* project on trans-jurisdictional disclosures of health information,[6] all jurisdictions currently send personal health information (in electronic and non electronic formats) across jurisdictional boundaries for care and treatment purposes.
For example:

- Residents in communities that straddle jurisdictional boundaries may receive care on both sides of the border
- Residents in rural and remote communities – residents of northern communities and territories in particular – travel to other jurisdictions for regular, non-specialized care and treatment
- Regional centres of excellence provide specialized services for the treatment of serious conditions – such as cancer treatment, cardiac care and organ transplants
- Medical services are provided to temporary residents
- Emergency department services are provided to out-of-jurisdiction visitors
- Files are transferred to another jurisdiction due to a change of residence
- Services, such as radiology services, or telehealth services, are provided by clinicians who reside in another jurisdiction
- Services are provided by clinicians who are temporarily outside of the jurisdiction (e.g., clinicians at conferences but continuing to follow their patients' treatments).

Information is also disclosed to other jurisdictions for secondary uses, notably research, but also for billing and related administrative purposes, public health surveillance, and other authorized secondary uses.

Currently, information in a non-electronic (paper, tape, verbal) or electronic (CD, flash drive, DVD, disc) format flows physically (carried by patient, telephone, post, courier) or semi-electronically (faxed) between jurisdictions. There are also examples of electronic information (such as radiology imaging and e-mail information) flowing electronically (via systems such as Picture Archiving and Communication systems (PACs) and secure e-mail and store-and-forward

[6] *Canada Health Infoway, Trans-jurisdictional Flows of EHR Data in Canada, v.2, July, 2009 http://www2.infoway-inforoute.ca/Documents/Trans-Jurisdictional_Flows_of_EHR_Data_in_Canada_v2.pdf*

systems) from an institution or medical office in one jurisdiction to an institution or medical office in another.

These flows or disclosures essentially reflect the existing environment, rather than the shift that the iEHR represents. Generally, the patient's care provider in the home jurisdiction chooses what information to disclose to the out-of-jurisdiction clinician. It could be a letter of introduction plus the patient's full file and results or it could be little more than a referral sheet.

Such disclosures are driven by medical imperatives and are often based on historical patterns established in a jurisdiction's health system. Some of these flows are governed by agreements between jurisdictions.

The iEHR world represents a different situation, one that is still evolving. It could be that, once the out-of-jurisdiction requestor is sufficiently authorized (via rules built into the system) the home jurisdiction's system could make visible (disclose) to the out-of-jurisdiction requestor an EHR screen (e.g., the shared record summary in the case of an emergency; or perhaps more detail if it is a specialist referral). Rather than being based on a one-to-one communication between clinicians, the disclosure could be transacted on the basis of rules built into the system related to the authority of the individual to request the information, the identification and authentication of the patient, the authority of the sending jurisdiction to make out-of-jurisdiction disclosures, the specific information in question and any rules that may be in place regarding masked or locked data. And it is possible that, rather than being comprised solely of the information the clinician chooses to disclose from the patient's file, the information disclosed could involve a series of standardized screens containing standard sets of information.

Trans-jurisdictional disclosures for secondary uses in the iEHR context are also expected to work quite differently. While potential scenarios are still in early stages, one given is that data for secondary uses will not be disclosed directly from the live iEHR or EHR and those seeking such information will not be provided access to live EHR systems. (See Section 2 for discussion of common understandings relating to secondary use of EHR data).

The following common understandings of the HIP Group support appropriate and privacy-protective trans-jurisdictional disclosures in this new iEHR context and are flexible enough to take into account the various approaches jurisdictions are taking to privacy and the development and implementation of their EHR systems. It is recognized that some of these common understandings may appear self-evident; however the HIP Group felt it important to include the following six foundational principles to set the stage for subsequent common understandings.

A) Foundational Principles

Support for appropriate and privacy-protective trans-jurisdictional disclosures within Canada

It is a common understanding that:

1. Jurisdictions support appropriate (i.e., authorized, necessary) and privacy-protective trans-jurisdictional disclosures of personal health information.

2. Jurisdictions make EHR technology/system choices that meet legislative requirements, while striving for pan-Canadian interoperability to support trans-jurisdictional disclosures.

EHR governance structures

It is a common understanding that:

3. For jurisdictions to be comfortable making disclosures of the personal health information of their residents to other jurisdictions, they require confidence in other jurisdictions' laws, regulations and practices that relate to how that personal health information will be handled and protected.[7] Jurisdictional EHR governance structures that include a privacy and information governance component are one element of this trust framework. (See Section 3 for a discussion of this issue.)

4. A pan-Canadian structure is also important for the coordination of information governance issues related to trans-jurisdictional disclosures of EHR information. (See Section 3 for further discussion.)

Authorities for disclosures to other jurisdictions within Canada

Each jurisdiction currently has a different mix of legislation, policy and precedent/practice governing its management of personal health information. This mix may include agreements or related tools that function in tandem with or in place of legislation (when legislation does not exist) to authorize disclosures. Personal health information is currently collected, used and disclosed within and across jurisdictions within this mix, and this will continue to be the case in the EHR context. Because most privacy and health information privacy legislation and associated policies are subject to regular review, the legal and policy framework evolves over time to take into account advances in privacy and other issues.

It is a common understanding that:

5. Jurisdictions disclose EHR information in compliance with the appropriate authority framework that may include legislation, policies (that provide guidance to legislation or act in the place of legislation where none exists) and agreements.

6. The longer-term vision is for each jurisdiction to have legislation and/or policies in place that clearly authorize appropriate trans-jurisdictional disclosures from the EHR, as well as the privacy and security of personal health information.

[7] *E.g., Quebec law prohibits disclosures to another jurisdiction if that jurisdiction does not have equivalent privacy protection of personal health information.*

B) *Trans-jurisdictional disclosure principles*

Disclosure principles

It is a common understanding that:

7. When a custodian or trustee in one jurisdiction provides personal health information to a custodian or trustee in a second jurisdiction, it is a disclosure from one jurisdiction and an (indirect) collection by the second jurisdiction, even if the information is only "viewed", but not recorded, in the second jurisdiction. (Note that this means that multiple custodians could have custody and/or[8] control over the same information in different jurisdictions.)

8. A disclosing jurisdiction must follow its legislation and policies for disclosure to a second jurisdiction, and the jurisdiction to which the information is disclosed must follow its legislation and policies for (indirect) collection.

9. Once information is disclosed to a custodian or trustee in a second jurisdiction (and thereby has been indirectly collected by a custodian or trustee in the second jurisdiction), it becomes subject to the information handling legislation and policies of the second jurisdiction.

10. All EHR information disclosed from a custodian or trustee in one jurisdiction to a custodian or trustee in a second jurisdiction should be protected by reasonable safeguards, and in compliance with applicable legislative requirements in the receiving jurisdiction, whether or not the information is recorded. Where legislation does not refer to unrecorded personal health information, such information may be protected by policy or by professional ethical obligations.

Identity management

As identified in a paper[9] examining trans-jurisdictional disclosures of information for care and treatment, the ability to unambiguously identify a patient and a provider involved in such disclosures is of great importance, not just from an operational perspective, but even more so, from the standpoint of privacy and patient safety. This issue is beyond the scope of this paper and needs to be addressed in a wider context; however, the common understanding that follows is intended to underscore its importance.

It is a common understanding that:

11. Processes should be in place for uniquely identifying patients and providers in trans-jurisdictional disclosures and collections of information.

[8] *The use of "and/or" reflects the existence of jurisdictional differences regarding custody and control*

[9] *Canada Health Infoway, Trans-jurisdictional Flows of EHR Data in Canada, v.2, July, 2009 http://www2.infoway-inforoute.ca/Documents/Trans-Jurisdictional_Flows_of_EHR_Data_in_Canada_v2.pdf*

C) Patient control of their personal health information

Respecting patient/individuals' wishes

It is a common understanding that:

12. As in the paper-based environment, jurisdictions recognize the value of including all relevant and necessary information in the EHR. Jurisdictions also support patients' rights to exercise a measure of control[10,11] over the use and disclosure of their personal health information for care and treatment, and strive to respect the control a patient has put on this information in trans-jurisdictional disclosures.

13. When a patient seeks care in another jurisdiction, whether in an emergency, for planned care or for another reason, the control a patient has exercised over his or her information in the home jurisdiction should be respected in the second jurisdiction to the extent possible given the legal framework and technology in use in the second jurisdiction:

- Except where otherwise permitted, if personal health information has been masked,[12] it should not be disclosed to another jurisdiction. In these situations, the care provider in the jurisdiction requesting the information must be advised that information has been masked and is not being disclosed.
- However, where permitted because the patient has provided consent or the situation meets a jurisdiction's override criteria, information may be unmasked and disclosed to the requesting jurisdiction. In these situations, both the disclosing and collecting jurisdictions should log the transactions. The collecting jurisdiction should make efforts to re-mask the information in accordance with its legal framework and technology currently in place in the jurisdiction, and the patient should be notified of the results.

[10] Jurisdictions use various terms – e.g., consent directives, disclosure directives, expressed wishes -- to describe how a patient can exercise the principle of patient control to restrict access to, use and/or disclosure of his or her personal health information. (Note: this relates to the INFORMATION in the record, not consent for treatment)

[11] Note that based on the current legislation in Quebec, patients have the right to opt out of the province's EHR, but if they participate, they do not have the right to mask any information in it.

[12] If legislative provisions allow for patient control and a request for masking has been made, but existing systems do not have the capability to support masking, the information should not be disclosed to another jurisdiction unless the patient has provided consent or the situation meets the jurisdiction's override criteria.

Patient information/notices about EHRs

In helping patients become well-informed about EHRs, jurisdictions must decide how much information to make available and how to best deliver the information. Jurisdictions wish to provide sufficient and relevant information to the patient in a way that does not hamper clinical workflow. The common understandings that follow seek to find the balance among these issues.

It is a common understanding that:

14. The information included in patient notices[13] is a jurisdiction's responsibility and will depend on its approach to health care delivery. Notices about the EHR should include information about trans-jurisdictional disclosures, in addition to information on topics such as, but not limited to the following:

- What information is collected
- The purpose of collection (i.e., for care and treatment) and whether that information may also be used for other purposes such as determining payment for services provided, health system analysis, quality assurance reviews, education and research, under specified conditions
- Who is authorized to see patient information
- How patient information will be protected
- That if patient information is disclosed to another jurisdiction, it will be subject to the second jurisdiction's information handling laws and policies, which may be different from the approach in the patient's home jurisdiction
- Where to go for more detailed information and how/where to register an inquiry or complaint, whether their complaint refers to an incident in their home jurisdiction or another jurisdiction in Canada.

15. Where jurisdictions have legislative provisions and their EHR systems are capable of offering patient control of their information, patient notices and discussions with a patient requesting masking should include the following messages:

- That patients have a right to request masking as well as unmasking of some or all of their information
- The clinical implications and other limits of masking
- How to request that their information be masked or unmasked
- In which situations, such as emergencies, that legislation or policy allows their information to be unmasked without their consent, and whether or not in these situations, their information will be remasked automatically or whether they need to request remasking

[13] *MacPherson, D. and R. Fraser, "Jurisdictional Scan of Patient Notices" http://www2.infoway-inforoute.ca/Documents/Jurisdictional_Scan_of_Patient_Notices_EN_FINAL.pdf*

- Which, if any, other provisions in law or policy (in the absence of legislation) can override personal masking requests, for example, that their unmasked information in de-identified form may be used for secondary purposes
- That if they seek care in another jurisdiction, their information will be subject to the second jurisdiction's masking policies, which may be different from the approach in the home jurisdiction.

16. Neither patients nor health care providers are expected to be experts about other jurisdictions' EHR systems or health information privacy laws. Jurisdictions will need to work together to put in place practical and simple processes to point patients and providers towards sources of information about the information handling laws and policies of other jurisdictions.

Section 2:

Trans-jurisdictional disclosures of EHR information for secondary uses

Section 2:
Trans-jurisdictional disclosures of EHR information for secondary uses

Context

The term 'secondary use' has been widely used to refer to the utilization of health information for any purpose other than the provision of direct care and treatment. Most[14] secondary uses of health information relate to work that benefits the health of Canadians, but not through direct care and treatment. Recently other terms have also come into play, most notably 'health system use', which denotes using health information for clinical program management (including quality improvement and decision support), health system management (e.g., analysis, planning, monitoring), population health surveillance, and research. This paper will continue to use the term 'secondary use'.

The value of using health information for secondary uses has long been recognized and legislatively authorized, irrespective of the presence of the EHR. These secondary uses have been shown to improve the health care experience, expand knowledge about disease, illness and treatment, strengthen the effectiveness and efficiency of health care delivery and support public health initiatives.

Disclosures of personal health information for secondary use must be made in compliance with legislative authorities. Health information and privacy statutes commonly list authorized disclosures for secondary uses that trustees or custodians have the discretion to make without the consent of the individual (although few statutes use the term 'secondary use';[15] instead using terms such as 'permitted uses' or 'authorized uses'). The lists of authorized uses and associated disclosures are relatively consistent across jurisdictions. Where lists are not specifically set out, the legislation may indicate that the information may be used or disclosed for a purpose that is consistent with the purpose for which it was collected.

In keeping with this longstanding recognition of the value and appropriateness of secondary use of health information, numerous Canadian commissions and reports (most recently, Romanow[16] and Kirby[17]) have affirmed that part of the value of the EHR initiative would be the potential for using the stored information for research and related purposes.

[14] *A few secondary uses of health information have little or no relation to healthcare and are authorized under other statutes. Examples of these include mandatory reporting of gunshot wounds in some jurisdictions or complying with a warrant or subpoena. This paper is not focusing on these secondary uses.*

[15] *Of note Federal Privacy legislation does not recognize this terminology.*

[16] *Romanow Q.C., Roy, J. Commissioner, Building on Values: The Future of Health Care in Canada, November 2002; Chapter 3, Information, Evidence & Ideas. pp. 75-89 http://www.cbc.ca/healthcare/final_report.pdf*

[17] *The Honourable Michael J Kirby, The Health of Canadians – The Federal Role, Final Report, Volume Six, Recommendations for Reform, October 2002, Part V, Chapter Ten http://www.parl.gc.ca/37/2/parlbus/commbus/senate/Com-e/soci-e/rep-e/repoct02vol6-e.htm*

Like care and treatment, most other uses of health information take place within a jurisdiction and this will continue to be the case in the EHR context. Jurisdictions, however, do currently disclose information to other jurisdictions for secondary uses, even though practical issues, such as allowing remote access only within the jurisdiction, can make such disclosures difficult to operationalize.[18] The EHR environment must continue to allow for the appropriate and privacy-protective use and disclosure of health information for secondary uses not only within, but also across jurisdictions.

(Note: this paper assumes that those seeking EHR information for purposes other than direct care and treatment of a patient will not be provided access to "live" data, that is, to the EHR itself or to point-of-service systems connected to the EHR.)

It bears repeating that although the focus is on trans-jurisdictional disclosures, some of the common understandings below speak to the jurisdictional level. In part this is because jurisdictions recognize the desirability of consistent practices at the jurisdictional level, and in part, it is because trust in other jurisdictions is required for trans-jurisdictional disclosures of information for secondary purposes.

Scope and terminology

The privacy of personal health information involved in secondary use is a complex topic being examined in many quarters. The HIP Group is limiting its examination to trans-jurisdictional disclosures without consent of EHR information that is identifiable or potentially re-identifiable (PHI or potential PHI), for clinical program management, health system administration and research. This scope is summarized below:

In scope	**Out of scope**
Trans-jurisdictional disclosures	Uses and disclosures within a jurisdiction
Disclosures without consent	Disclosures for which consent is required or sought
EHR information	Information from source systems
Information that is identifiable or potentially re-identifiable – PHI or potential PHI	Anonymous or aggregated information
Clinical program management, health system administration and research	Population health surveillance Secondary uses unrelated to health

Within this scope, the HIP Group's focus is on de-identification of personal health information, review and assessment processes, patient notification and governance.

[18] *El Emam, K, Practices for the Review of Data Requests and the Disclosure of Health Information by Health Ministries and Large Data Custodians. http://www2.infoway-inforoute.ca/Documents/Practices_for_the_review_of_data_requests_June_2010_EN_FINAL.pdf*

De-identification of personal health information

The disclosure of identifiable information – information that on its own or in combination with other available information could identify an individual – raises privacy risks. Privacy concerns diminish as information becomes increasingly unidentifiable.

There is a spectrum of identifiability that illustrates a gray zone rather than a sharp cut-off between what is identifiable and what is truly de-identified. One aspect of the spectrum has to do with the format of the information – record level information is data at the level of an individual person, and even if these data do not directly identify the person, they are more vulnerable than aggregate data, which are data that have been averaged or grouped into ranges across multiple records. The following illustrates three basic levels of the identifiability spectrum.

Identifiable information is:

- information that includes data elements that directly identify an individual, such as name, health number, etc., or
- record-level information that includes data elements such as full postal code, gender, date of birth and/or unique occupation, that in combination can be readily used to identify an individual even when direct identifiers such as name, have been removed.

Information is de-identified when:

- direct identifiers have been removed (or replaced with pseudonyms), and
- data elements that could be used to identify an individual, such as postal code, gender and date of birth, have been removed, generalized (e.g., removing the last three digits of a postal code), put into ranges (e.g., 10-year age category) or otherwise manipulated with the intent that the information not be re-identifiable, and
- no other data set can reasonably be expected to be available to combine with the data and re-identify the individual.

Information is anonymous when, for example:

- it is aggregated, and
- the aggregation satisfies rules about small cell size,[19] and
- no other data set can reasonably be expected to be available to combine with the data and re-identify the individual.

[19] *Aggregate information that does not meet aggregation rules about small cell size is potentially identifiable*

It is a common understanding that:

17. Trans-jurisdictional disclosures for secondary uses should, as a general rule, involve aggregated or de-identified information. The disclosing jurisdiction is responsible for the aggregation or de-identification procedures before disclosing the information.

18. In some situations legislation authorizes or requires the disclosure of identifiable information.[20]

As outlined in a paper[21] on de-identification tools prepared for the HIP Group, ever increasing computing power and availability of online databases for data linkage make it more and more difficult to de-identify information with confidence that the potential for re-identification is low, while keeping its informative value for analysis and research. The paper describes a number of tools that are available to de-identify information. The use of the tools, however, requires considerable technical and statistical expertise and it does not appear that they are consistently or widely used at this time.

It is a common understanding that:

19. Those entities and individuals responsible for handling requests for trans-jurisdictional disclosures of EHR information for secondary uses should be knowledgeable about de-identification, up-to-date on de-identification tools and techniques, and able to apply them.

Even when de-identification tools are used, it will still be necessary to assess the risk of the proposed disclosure and to outline the responsibilities and obligations of the data requestor. This is particularly important since de-identification and re-identification techniques and strategies are constantly evolving, and it is therefore not possible to guarantee that de-identified data will never be able to be re-identified.

It is a common understanding that:

20. De-identification techniques should work hand in hand with risk assessment processes,[22] agreements (which set out obligations and conditions for management of health information being used for secondary purposes), security practices and other safeguards to minimize the privacy risks of disclosing information for secondary uses.

[20] *For example, Ontario's PHIPA authorizes such disclosures.*

[21] *Fraser, R. and D. Willison, "Tools for De-Identification of Personal Health Information" http://www2.infoway-inforoute.ca/Documents/Tools_for_De-identification_EN_FINAL.pdf*

[22] *Ibid.*

Review and assessment processes in trans-jurisdictional disclosure requests

The EHR system will hold ever increasing volumes of personal health information and trans-jurisdictional requests for portions of that information for research and other secondary uses (including those that are not related to health care) can be expected to increase over time. The potential for supporting valuable research is great but so too are the potential privacy risks.

It is a common understanding that:

21. Jurisdictions need to put in place processes to enable appropriate and privacy protective trans-jurisdictional disclosures of EHR data for secondary uses. It is recognized that some jurisdictions may not have the capacity to undertake these processes, and could work with other jurisdictions or bodies in this regard.

Custodians of EHR holdings will need to manage trans-jurisdictional requests for EHR information for secondary uses and their risks in a manner that engenders trust with the public. Robust and sensitive reviews of such requests can help to strike the balance between protecting the privacy of individuals, and providing requesters useful information for activities that will benefit Canadians in general.

It is a common understanding that:

22. Requests for disclosure of identifiable or potentially re-identifiable information from the EHR to individuals or organizations in another jurisdiction for research, clinical program management and health system administration, should, in addition to complying with Research Ethics Board processes, undergo an assessment of privacy risks at the outset and as required over time. Special consideration should be given to requests for readily identifiable data or for record-level data (individual records), to ensure the need for such data is authorized and justified.

23. The formality of the assessment process should be commensurate to the potential privacy risk related to the project at hand.

The completion of a questionnaire or checklist may be sufficient to assess projects whose privacy risks appear minimal, while a more formal process may be required for one where the privacy risks appear more substantial. For example, the review of requests for disclosure of particularly sensitive information, such as information about abortion procedures, is likely to require a more in-depth review than a request for disclosure of aggregate information about diabetes treatment regimes. Part of the goal of the process is to embed an organizational and cultural predisposition towards considering privacy at the outset of any potential trans-jurisdictional disclosures of EHR information.

Ideally, processes should be consistent across the country. Various risk assessment tools and processes already exist,[23] including Alberta's Alberta Research Ethics Community Consensus Initiative (ARECCI) guidelines[24] and the Privacy Analytics Re-identification Risk Assessment and De-identification Tool.[25] High level core elements of an assessment process would include:

- Understanding of the project and purpose of the disclosure
- Compliance with legislative, policy or other authorities and requirements for the disclosure for secondary use
- Existence of and conformity with a data sharing or similar agreement or arrangement
- Correspondence of the information requested to that needed for the purpose
- Identifiability of the information requested
- Sensitivity of the information (extent to which its exposure could cause harm, embarrassment, etc. to an individual or group)
- Potential for exposure of the information (e.g., level of de-identification, potential for linkage with other datasets for re-identification, data security; access controls)
- Risk management elements (e.g., how data will be disclosed (e.g., on-site or remote access) requirement for review of final products or outputs, compliance audits).

[23] *Ibid.*

[24] *These guidelines assist in the determination of whether or not a project should be considered "research" (and subject to a REB) and also assess the privacy risk for both research and non-research (quality assurance and evaluation-type projects)* http://www.ahfmr.ab.ca/arecci/screening/

[25] *http://www.ehealthinformation.ca/index.asp*

Patient notification respecting trans-jurisdictional disclosures for secondary uses

It is a common understanding that:

24. Patient notices should include general information on trans-jurisdictional disclosures of information for secondary uses.

More information should also be available to patients wishing more detail. Relevant messages include:

- Examples of the types of trans-jurisdictional disclosures that are made for secondary uses
- Legislation which allows for these disclosures without seeking patient consent
- That information disclosed for these secondary uses is generally de-identified
- That even if patients have masked their identifiable information, the information in de-identified form may be disclosed to another jurisdiction for secondary uses
- That patients have a right to ask for a report of the trans-jurisdictional disclosures that have been made of their identifiable information for secondary uses
- That once the information is in a second jurisdiction it is subject to the data protection provisions of the second jurisdiction.

It is a common understanding that:

25. Records must be kept of trans-jurisdictional disclosures of identifiable information for secondary uses so that reports can be made to a patient upon request.

Governance of trans-jurisdictional disclosures for secondary uses

Although legislatively authorized disclosures for secondary uses are somewhat consistent across jurisdictions, there are some differences in legislation and practice which may have an impact on disclosing EHR information to another jurisdiction for secondary purposes.

For example, British Columbia's *Freedom of Information and Protection of Privacy Act* allows the disclosure by public bodies of residents' data outside the country for specific purposes only, while the *E-Health (Personal Health Information Access and Protection) Act* only allows the disclosure outside of Canada to assess and address threats to public health. The province expects these restrictions to be respected should the data of BC residents be disclosed to another jurisdiction in Canada. In Nova Scotia, the *Personal Information International Disclosure Protection Act* restricts the ability of a public body to access or store personal information outside of the country unless certain conditions are met. Jurisdictions will need to determine if their restrictions can be formally or informally imposed on a collecting jurisdiction.

It is a common understanding that:

26. Jurisdictions must comply with their statutes and policies before disclosing EHR information to other jurisdictions for secondary uses, and for collecting information from another jurisdiction.

27. Once the information is collected by another jurisdiction, the information handling rules in the collecting jurisdiction take effect.

Agreements are one of the tools available to help bridge differing approaches among jurisdictions and provide confidence in making disclosures of EHR information across borders in Canada. Such agreements set out legislative authority and obligations, manage risk, define due diligence and manage service expectations. A paper prepared for the HIP Group discusses these types of agreements and provides samples and templates.[26]

It is a common understanding that:

28. Agreements setting out the rules under which information is to be disclosed to another jurisdiction for secondary uses should be in place to formalize recurring and ad hoc disclosures of EHR information for these uses. Such agreements may provide details not set out in legislation or provide guidance in the absence of legislation.

An agreement between jurisdictions should include, among other elements:

- Purpose of the agreement
- Legislative or other authorities for the agreement and for the information disclosure and subsequent collection
- Allowable information uses and processing covered by the agreement, and any restrictions, such as onward disclosures
- The identification of accountable bodies or persons
- Level of identifiability of the information being disclosed
- Any further uses or onward disclosures of the information that are or are not authorized, for example, data linkage protocols
- The controls to which the information is subject, such as privacy risk assessments, security measures and audit provisions
- Process requirements, such as the term of the agreement and program changes that trigger a review of the agreement.

As noted above, there is a desire for some degree of consistency across Canada in practices and processes around disclosures for secondary use. Moreover, as experience grows with trans-jurisdictional disclosures of EHR information for secondary uses, it is expected that new issues will arise.

It is a common understanding that:

29. Issues around secondary uses of EHR information would benefit from pan-Canadian deliberation and the development of recommendations for consideration by all jurisdictions in an effort to promote a degree of consistency in approach across the country.

[26] *Sawatsky, Elaine, "Information Sharing Agreements for Disclosure of EHR Data Within Canada" http://www2.infoway-inforoute.ca/Documents/ISA_report_for_HIP_Group_January_2010_EN_Final.pdf*

Section 3:

Accountability for information governance in the EHR

Section 3:
Accountability for information governance in the EHR

This section of the paper focuses on the principle of accountability in relation to privacy of personal health information held in the EHR. In this context, accountability refers to responsibility for decisions related to the collection, access (in all the senses of the term), use, disclosure, retention and overall protection of personal health information. It encompasses patients' access to their own information and accountability to the patient for the protection of his or her personal health information; as well as accountability to a Minister or other body for the good management of information in the iEHR.

Accountability at the jurisdictional level

Health information and general privacy legislation in most Canadian jurisdictions identify who can be a custodian (or trustee or other term) and the obligations of a custodian. These statutes also generally require that a body authorized as a custodian identify an individual to be accountable for compliance with the privacy-related obligations set out in the statutes. Jurisdictions also have oversight bodies which are mandated to protect privacy rights and to oversee compliance with jurisdictional privacy legislation.

Ministers of Health (or equivalents[27]) are ultimately responsible for the delivery of health services within their boundaries, for the EHR being created to support health service delivery and for the management of information that will be collected and stored in the EHR systems. However many bodies, such as health authorities, hospitals and individual health care providers, are accountable for those individual parts of the overall EHR system over which they have control. In an interoperable EHR environment, such control can be more complicated to identify because:

- health information from multiple custodians can be held in a single repository
- health information stored in the repositories may be transformed to agreed upon coding structures
- information stored in the repositories may be accessed by multiple providers.

[27] *This is to ensure appropriate representation of federal departments, such as DND or VAC which deliver health services but do not report to a Minister of Health.*

Jurisdictions are taking a variety of approaches as they deem appropriate to their EHR governance structures and accountability. (Appendix B illustrates examples of various jurisdictional EHR accountability structures.) Some have centralized models, others are decentralized; they may be based within or outside a ministry. Some jurisdictions may be covered by another jurisdiction's EHR and EHR governance structure. Yet some common themes are emerging, for example:

- Consensus-building through consultation and stakeholder involvement
- Information governance through, for example, data stewardship committees
- Transparency through steering committees or councils
- Reporting to government from arm's length organization or committees
- Flexibility to allow for evolution over time.

It is a common understanding that:

30. Whatever approach is taken to overall governance of a jurisdiction's EHR:

    - It should include a privacy and information governance component
    - It should be ultimately accountable to the Minister of Health/e-Health or equivalent and have some form of formal standing – e.g., established via Ministerial authority, Order, legislation, etc.
    - It should be clearly articulated where accountability resides for the EHR system as a whole and its parts so that patients, providers and oversight bodies within and outside the jurisdiction know to whom they can turn if they wish to access their own information or make a correction to it, or if they encounter a problem.

The HIP Group believes that the privacy and information governance component could have responsibilities that include, in compliance with legislation and policy:

- Setting and ensuring compliance with policies and rules for collection, access, use, disclosure and retention of PHI in the EHR
- Exercising authority for decisions related to the secondary uses of information within the jurisdiction in a transparent fashion, setting policy directions for secondary uses and being responsible for compliance with the body's decisions by recipients of EHR data for secondary purposes
- Advising the ministry on or negotiating on behalf of/in collaboration with the ministry, information sharing agreements with other jurisdictions for trans-jurisdictional disclosures and collections of EHR information
- Setting common requirements for information sharing/manager agreements or other tools
- Serving as the breach investigation coordinator in situations where the source of a breach is unclear or involves multiple sources. This could include notifying patients as required or appropriate, and notifying the relevant oversight body as required
- Maintaining up-to-date standards and jurisdictional practices relating to privacy and security, as well as information technology related to the EHR

- Representing the jurisdiction on any pan-Canadian body for EHR privacy and related information governance, serving as a point of contact between jurisdictions for discussion of certain issues and liaising with oversight bodies
- Acting as a resource for organizations in privacy and information governance issues for the EHR
- Responding to patient complaints and patient access requests related to the EHR that cannot be dealt with or have been escalated by the entity or entities concerned
- Managing public education initiatives, for example, serving as the coordinating body for patient notification templates, best practices, etc., and engaging the public in the continuing development and refinement of the EHR.

Accountability at the organizational level

Within jurisdictions, organizations, (including points of service, entities, custodians, facilities, providers, registries and others) collect, use and disclose personal health information in accordance with specific policies and procedures that comply with jurisdictional laws and policies. Many of these organizations are the primary point of contact for patients regarding privacy issues.

Organizations are generally required (by law or policy) to have a process for overall privacy compliance, including dealing with individual complaints, as well as with requests for access to personal health information by the individual and the correction of errors.

It is a common understanding that:

31. Organizations should revisit their privacy compliance process in the EHR context to ensure that it remains transparent and accessible to patients/clients and providers. Organizations also need to revisit their privacy roles and responsibilities, for example:

   - Ensuring that patients are provided contact information for persons who can respond to their privacy questions or complaints related to the EHR
   - Exercising operational responsibility for staff, training and the implementation of policies and procedures for technical, physical and administrative safeguards for the protection of personal health information in the EHR[28]
   - Complying with jurisdictional legislation and policy, proposed secondary uses and disclosures of personal health information from the EHR
   - Establishing clear relationships with the jurisdictional EHR governance structure.

[28] *The Canadian Medical Protective Association has, for example, issued an Electronic Records Handbook to provide members with an overview of the issues associated with EHRs and EMRs. It can be downloaded at* http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_records_handbook-e.cfm

Accountability and trans-jurisdictional disclosures of personal health information

The matter of accountability can be even more challenging when EHR health information is disclosed from one jurisdiction to another. In the trans-jurisdictional context it must be recognized that jurisdictional statutes differ, that one jurisdiction's laws do not have power in another jurisdiction, and that disclosures for care and treatment as well as for secondary uses can be expected to increase over time. Despite the complexity of the EHR environment, patients, providers, and oversight bodies still need to know:

- who is accountable for the information systems
- to whom the individual patient can turn if they wish access to their own information
- who is responsible for investigating and resolving any problems that arise.

The common understandings in this paper address some but not all of the issues related to supporting appropriate and privacy-protective trans-jurisdictional disclosures, and it is expected that as time goes on, new trans-jurisdictional issues will arise needing coordination across jurisdictions. Since privacy needs to be embedded in every aspect of the EHR, architects, subject matter experts in privacy, security specialists and other information technology specialists need to work together on these issues so that each can bring their particular expertise to the table.

It is a common understanding that:

32. Even though accountability for the privacy of personal health information held in the EHR will continue to rest with the jurisdictions, a pan-Canadian coordinating group is needed to discuss, address and coordinate common information governance issues including those related to trans-jurisdictional disclosures/collections of information. Such a group will continue to be needed as the EHR is rolled out and maintained across the country.

33. The group should be a single integrated structure that brings together the many specializations (including but not limited to expertise in privacy, security, and related IT issues and standards) needed to manage information and information technologies in a privacy sensitive manner and to create a culture of privacy that will engender the trust and support of patients, clinicians and the public at large in the EHR system.

The current HIP Group, whose establishment was supported by jurisdictional Deputy Ministers, includes the core representation and activities of such a pan-Canadian structure. The mandate of the HIP Group, however, focuses on discussion and information sharing, rather than on addressing and coordinating issues. There is a need for further discussion about the potential evolution of the HIP Group's mandate and composition. Appendix C illustrates a range of options that could be considered by jurisdictions as a starting point for discussions. In the meantime, the current HIP Group will move on to consider additional topics in information governance of the iEHR.

Appendix A: Summary List of Common Understandings

Section 1: Pan-Canadian common understandings to support trans-jurisdictional disclosures of EHR information within Canada

A) Foundational Principles

It is a common understanding that:

1. Jurisdictions support appropriate (i.e., authorized, necessary) and privacy-protective trans-jurisdictional disclosures of personal health information. (Page 13)

2. Jurisdictions make EHR technology/system choices that meet legislative requirements, while striving for pan-Canadian interoperability to support trans-jurisdictional disclosures. (Page 13)

3. For jurisdictions to be comfortable making disclosures of the EHR personal health information of their residents to other jurisdictions, they require confidence in other jurisdictions' laws, regulations and practices that relate to how that personal health information will be handled and protected.[29] Jurisdictional EHR governance structures that include a privacy and information governance component are one element of this trust framework. (See Section 3 for a discussion of this issue.) (Page 14)

4. A pan-Canadian structure is also important for the coordination of information governance issues related to trans-jurisdictional disclosures of EHR information. (See Section 3 for further discussion.) (Page 14)

5. Jurisdictions disclose EHR information in compliance with the appropriate authority framework that may include legislation, policies (that provide guidance to legislation or act in the place of legislation where none exists) and agreements. (Page 14)

6. The longer-term vision is for each jurisdiction to have legislation and/or policies in place that clearly authorize appropriate trans-jurisdictional disclosures from the EHR, as well as the privacy and security of personal health information. (Page 14)

[29] *E.g., Quebec law prohibits disclosures to another jurisdiction if that jurisdiction does not have equivalent privacy protection of personal health information.*

B) Trans-jurisdictional disclosure principles

It is a common understanding that:

7. When a custodian or trustee in one jurisdiction provides personal health information to a custodian or trustee in a second jurisdiction, it is a disclosure from one jurisdiction and an (indirect) collection by the second jurisdiction, even if the information is only "viewed", but not recorded, in the second jurisdiction. (Note this means that multiple custodians could have custody and/or control of the same information in different jurisdictions.) (Page 15)

8. A disclosing jurisdiction must follow its legislation and policies for disclosure to a second jurisdiction, and the jurisdiction to which the information is disclosed must follow its legislation and policies for (indirect) collection. (Page 15)

9. Once information is disclosed to a custodian or trustee in a second jurisdiction (and thereby has been indirectly collected by a custodian or trustee in the second jurisdiction), it becomes subject to the information handling legislation and policies of the second jurisdiction. (Page 15)

10. All EHR information disclosed from a custodian or trustee in one jurisdiction to a custodian or trustee in a second jurisdiction should be protected by reasonable safeguards, and in compliance with applicable legislative requirements in the receiving jurisdiction, whether or not the information is recorded. Where legislation does not refer to unrecorded personal health information, such information may be protected by policy or by professional ethical obligations. (Page 15)

11. Processes should be in place for uniquely identifying patients and providers in trans-jurisdictional disclosures and collections of information. (Page 15)

C) Patient control of their personal health information

12. As in the paper-based environment, jurisdictions recognize the value of including all relevant and necessary information in the EHR. Jurisdictions also support patients' rights to exercise a measure of control[30,31] over the use and disclosure of their personal health information for care and treatment, and strive to respect the control a patient has put on this information in trans-jurisdictional disclosures. (Page 16)

[30] *Jurisdictions use various terms – e.g., consent directives, disclosure directives, expressed wishes -- to describe how a patient can exercise the principle of patient control to restrict access to, use and/or disclosure of his or her personal health information. (Note: this relates to the INFORMATION in the record, not consent for treatment)*

[31] *Note that based on the current legislation in Quebec, patients have the right to opt out of the province's EHR, but if they participate, they do not have the right to mask any information in it.*

13. When a patient seeks care in another jurisdiction, whether in an emergency, for planned **care or for another reason, the control a patient has exercised over his or her information in** the home jurisdiction should be respected in the second jurisdiction to the extent possible given the legal framework and technology in use in the second jurisdiction:

- Except where otherwise permitted, if personal health information has been masked,[32] it should not be disclosed to another jurisdiction. In these situations, the care provider in the jurisdiction requesting the information must be advised that information has been masked and is not being disclosed.
- However, where permitted because the patient has provided consent or the situation meets a jurisdiction's override criteria, information may be unmasked and disclosed to the requesting jurisdiction. In these situations, both the disclosing and collecting jurisdictions should log the transactions. The collecting jurisdiction should make efforts to re-mask the information in accordance with its legal framework and technology currently in place in the jurisdiction, and the patient should be notified of the results. (Page 16)

14. The information included in patient notices[33] is a jurisdiction's responsibility and will depend on its approach to health care delivery. Notices about the EHR should include information about trans-jurisdictional disclosures, in addition to information on topics such as, but not limited to the following:

- What information is collected
- The purpose of collection (i.e., for care and treatment) and whether that information may also be used for other purposes such as determining payment for services provided, health system analysis, quality assurance reviews, education and research, under specified conditions
- Who is authorized to see patient information
- How patient information will be protected
- That if patient information is disclosed to another jurisdiction, it will be subject to the second jurisdiction's information handling laws and policies, which may be different from the approach in patient's home jurisdiction
- Where to go for more detailed information and how/where to register an inquiry or complaint, whether their complaint refers to an incident in their home jurisdiction or another jurisdiction in Canada. (Page 17)

[32] *If legislative provisions allow for patient control and a request for masking has been made, but existing systems do not have the capability to support masking, the information should not be disclosed to another jurisdiction unless the patient has provided consent or the situation meets the jurisdiction's override criteria.*

[33] *MacPherson, D. and R. Fraser, "Jurisdictional Scan of Patient Notices" http://www2.infoway-inforoute.ca/Documents/Jurisdictional_Scan_of_Patient_Notices_EN_FINAL.pdf*

15. Where jurisdictions have legislative provisions and their EHR systems are capable of offering patient control of their information, patient notices and discussions with a patient requesting masking should include the following messages:

- That patients have a right to request masking as well as unmasking of some or all of their information
- The clinical implications and other limits of masking
- How to request that their information be masked or unmasked
- In which situations, such as emergencies, that legislation or policy allows their information to be unmasked without their consent, and whether or not in these situations, their information will be remasked automatically or whether they need to request remasking
- Which, if any, other provisions in law or policy (in the absence of legislation) can override personal masking requests, for example, that their unmasked information in de-identified form may be used for secondary purposes
- That if they seek care in another jurisdiction, their information will be subject to the second jurisdiction's masking policies, which may be different from the approach in the home jurisdiction. (Page 17)

16. Neither patients nor health care providers are expected to be experts about other jurisdictions' EHR systems or health information privacy laws. Jurisdictions will need to work together to put in place practical and simple processes to point patients and providers towards sources of information about the information handling laws and policies of other jurisdictions. (Page 18)

Section 2:
Trans-jurisdictional disclosures of EHR information for secondary uses

De-identification of personal health information

It is a common understanding that:

17. Trans-jurisdictional disclosures for secondary uses should, as a general rule, involve aggregate or de-identified information. The disclosing jurisdiction is responsible for the aggregation or de-identification procedures before disclosing the information. (Page 23)

18. In some situations legislation authorizes or requires the disclosure of identifiable information.[34] (Page 23)

19. Those entities and individuals responsible for handling requests for trans-jurisdictional disclosures of EHR information for secondary uses should be knowledgeable about de-identification, up-to-date on de-identification tools and techniques, and able to apply them. (Page 23)

20. De-identification techniques should work hand in hand with risk assessment processes,[35] agreements (which set out obligations and conditions for management of health information being used for secondary purposes), security practices and other safeguards to minimize the privacy risks of disclosing information for secondary uses. (Page 23)

Review and assessment processes in trans-jurisdictional disclosure requests

It is a common understanding that:

21. Jurisdictions need to put in place processes to enable the appropriate and privacy protective trans-jurisdictional disclosures of EHR data for secondary uses. It is recognized that some jurisdictions may not have the capacity to undertake these processes, and could work with other jurisdictions or bodies in this regard. (Page 24)

22. Requests for disclosure of identifiable or potentially re-identifiable information from the EHR to individuals or organizations in another jurisdiction for research, clinical program management and health system administration, should, in addition to complying with Research Ethics Board processes, undergo an assessment of privacy risks at the outset and as required over time. Special consideration should be given to requests for readily identifiable data or for record-level data (individual records), to ensure the need for such data is authorized and justified. (Page 24)

23. The formality of the assessment process should be commensurate to the potential privacy risk related to the project at hand. (Page 24)

[34] *For example, Ontario's PHIPA authorizes such disclosures.*

[35] *Fraser, R. and D. Willison, "Tools for De-Identification of Personal Health Information" http://www2.infoway-inforoute.ca/Documents/Tools_for_De-identification_EN_FINAL.pdf*

Patient notification respecting trans-jurisdictional disclosures for secondary use

It is a common understanding that:

24. Patient notices should include general information on trans-jurisdictional disclosures of information for secondary uses. (Page 26)

25. Records must be kept of trans-jurisdictional disclosures of identifiable information for secondary uses so that reports can be made to a patient upon request. (Page 26)

Governance of trans-jurisdictional disclosures for secondary use

It is a common understanding that:

26. Jurisdictions must comply with their statutes and policies before disclosing EHR information to other jurisdictions for secondary uses, and for collecting information from another jurisdiction. (Page 26)

27. Once the information is collected by another jurisdiction, the information handling rules in the collecting jurisdiction take effect. (Page 27)

28. Agreements setting out the rules under which information is to be disclosed to another jurisdiction for secondary uses should be in place to formalize recurring and ad hoc disclosures of EHR information for these uses. Such agreements may provide details not set out in legislation or provide guidance in the absence of legislation. (Page 27)

29. Issues around secondary uses of EHR information would benefit from pan-Canadian deliberation and the development of recommendations for consideration by all jurisdictions in an effort to promote a degree of consistency in approach across the country. (Page 27)

Section 3:
Accountability for information governance in the EHR

Accountability at the jurisdictional level

It is a common understanding that:

30. Whatever approach is taken to overall governance of a jurisdiction's EHR:

- It should include a privacy and information governance component
- It should be ultimately accountable to the Minister of Health/e-Health or equivalent and have some form of formal standing – e.g., established via Ministerial authority, Order, legislation, etc.
- It should be clearly articulated where accountability resides for the EHR system as a whole and its parts so that patients, providers and oversight bodies within and outside the jurisdiction know to whom they can turn if they wish to access their own information or make a correction to it, or if they encounter a problem. (Page 30)

Accountability at the organizational level

It is a common understanding that:

31. Organizations should revisit their privacy compliance process in the EHR context to ensure that it remains transparent and accessible to patients/clients and providers. Organizations also need to revisit their privacy roles and responsibilities. for example:

- Ensuring that patients are provided contact information for persons who can respond to their privacy questions or complaints related to the EHR.
- Exercising operational responsibility for staff, training and the implementation of policies and procedures for technical, physical and administrative safeguards for the protection of personal health information in the EHR.[36]
- Complying with jurisdictional legislation and policy, proposed secondary uses and disclosures of personal health information from the EHR.
- Establishing clear relationships with the jurisdictional EHR governance structure. (Page 31)

[36] *The Canadian Medical Protective Association has, for example, issued an Electronic Records Handbook to provide members with an overview of the issues associated with EHRs and EMRs. It can be downloaded at* http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_records_handbook-e.cfm

Accountability and trans-jurisdictional disclosures of personal health information

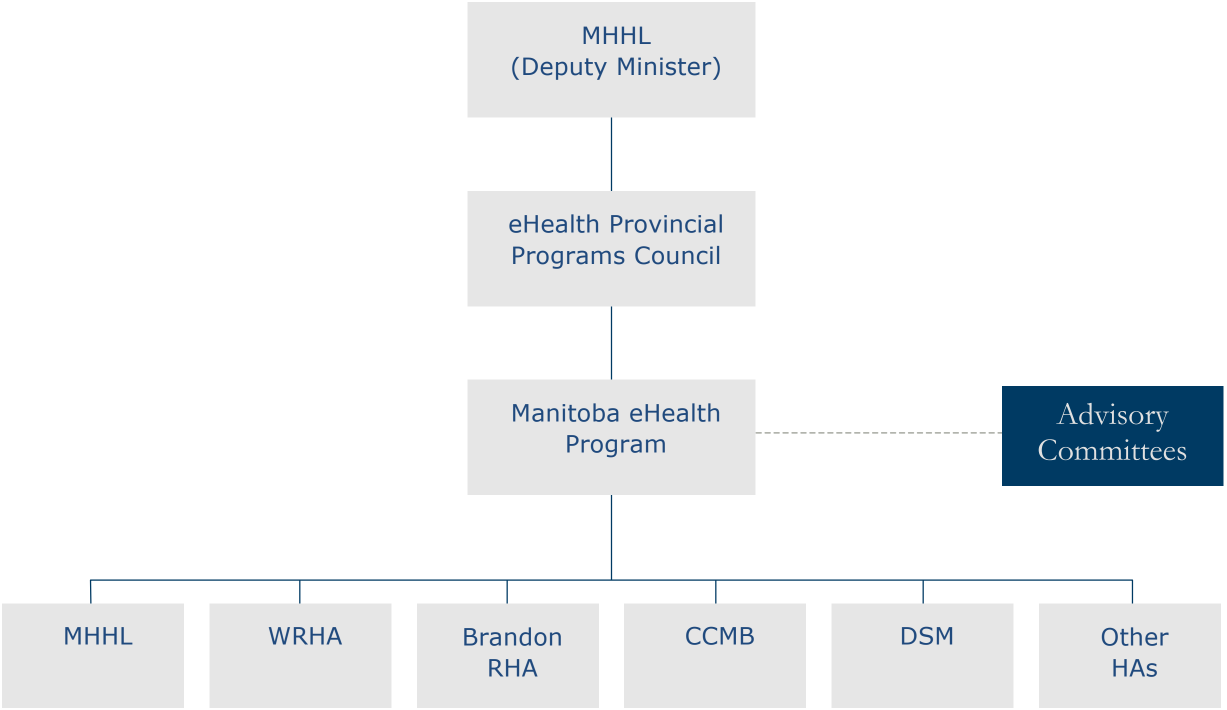
It is a common understanding that:

32. Even though accountability for the privacy of personal health information held in the EHR will continue to rest with the jurisdictions, a pan-Canadian coordinating group is needed to discuss, address and coordinate common information governance issues including those related to trans-jurisdictional disclosures/collections of information. Such a group will continue to be needed as the EHR is rolled out and maintained across the country. (Page 32)

33. The group should be a single integrated structure that brings together the many specializations (including but not limited to expertise in privacy, security, and related IT issues and standards) needed to manage information and information technologies in a privacy sensitive manner and to create a culture of privacy that will engender the trust and support of patients, clinicians and the public at large in the EHR. (Page 32)

Appendix B:
Examples of Jurisdictional EHR Governance Models

MANITOBA EHEALTH PROGRAM GOVERNANCE (2009)



Manitoba eHealth Program governance (2009)

The Manitoba eHealth Program reports to the Deputy Minister through a *Provincial Program Council* that is composed of senior executives of the major stakeholders as shown in the above chart.[37] The Council was first created in late 2008 and has 8 members – the CEOs of the six stakeholders, the Assistant Deputy Minister responsible for Corporate Programs at Manitoba Health and the CIO of the Manitoba eHealth Program.

The Program is administratively housed within the Winnipeg Regional Health Authority (WRHA), and is subject to all WRHA policies and processes. The CIO has a direct reporting line to the WRHA through its Chief Operating Officer, as well as to the Deputy Minister through the Council.

[37] *MHHL = Manitoba Health and Healthy Living; WRHA = Winnipeg Regional Health Authority; CCMB = CancerCare Manitoba; DSM = Diagnostic Services Manitoba; HA = Health Authorities*

Advisory committees

Telehealth and EHR Services

The developing Telehealth and EHR Services portfolio is being supported by three separate advisory committees: Registry Integrity Unit Advisory Committee; Primary Care Information System Advisory Committee; and the MBTelehealth Provincial Strategy and Investment Committee. In each committee stakeholders assist with input into key program decisions and ensure that services being developed are relevant to the key program users.

eHealth Clinician & Research Committees

- **eHealth Clinical Advisory Committee**
  Mandate: to provide advice and counsel to Manitoba eHealth regarding clinical applications
  Membership: 40 member group including 20 physicians
- **eHealth Research Advisory Committee**
  Mandate: to advise Manitoba eHealth regarding access to health care information for
  secondary use
  Membership: 16 member group including representatives from the University of Manitoba and the MCHP
- **Clinical Design Team**
  Mandate: to provide input into the clinical content of the EPR including Order Sets and Alerts
  Membership: diverse
- **Physician Champions**
  Mandate: to provide local expertise and liaise with respective institutions and programs
  Membership: 3 physicians
- **Core Clinical Design Team**
  Mandate: to establish regional principles regarding clinical content in the EPR application.
  Chair: Manager, Nursing Informatics Strategy, Manitoba eHealth

Privacy and security

The Privacy and Security Advisory Committee is responsible for providing recommendations on privacy and security matters related to the provincial iEHR and other Manitoba eHealth provincial projects.

The intent of the Provincial Privacy and Security Advisory Committee is to support the appropriate sharing of personal health information where and when required in a manner that protects the confidentiality, privacy, security and integrity of that information in accordance with *The Personal Health Information Act (PHIA).*

The membership includes privacy officers representing urban and rural regional health authorities, the Director of the provincial Information Protection Centre, an internal auditor, a clinician, a representative from Manitoba Health. A representative from the provincial Ombudsman's Office attends meetings as an observer.

Standards

Two committees govern standards: The Provincial Information Standards Committee and the Provincial Architecture Management Committee.

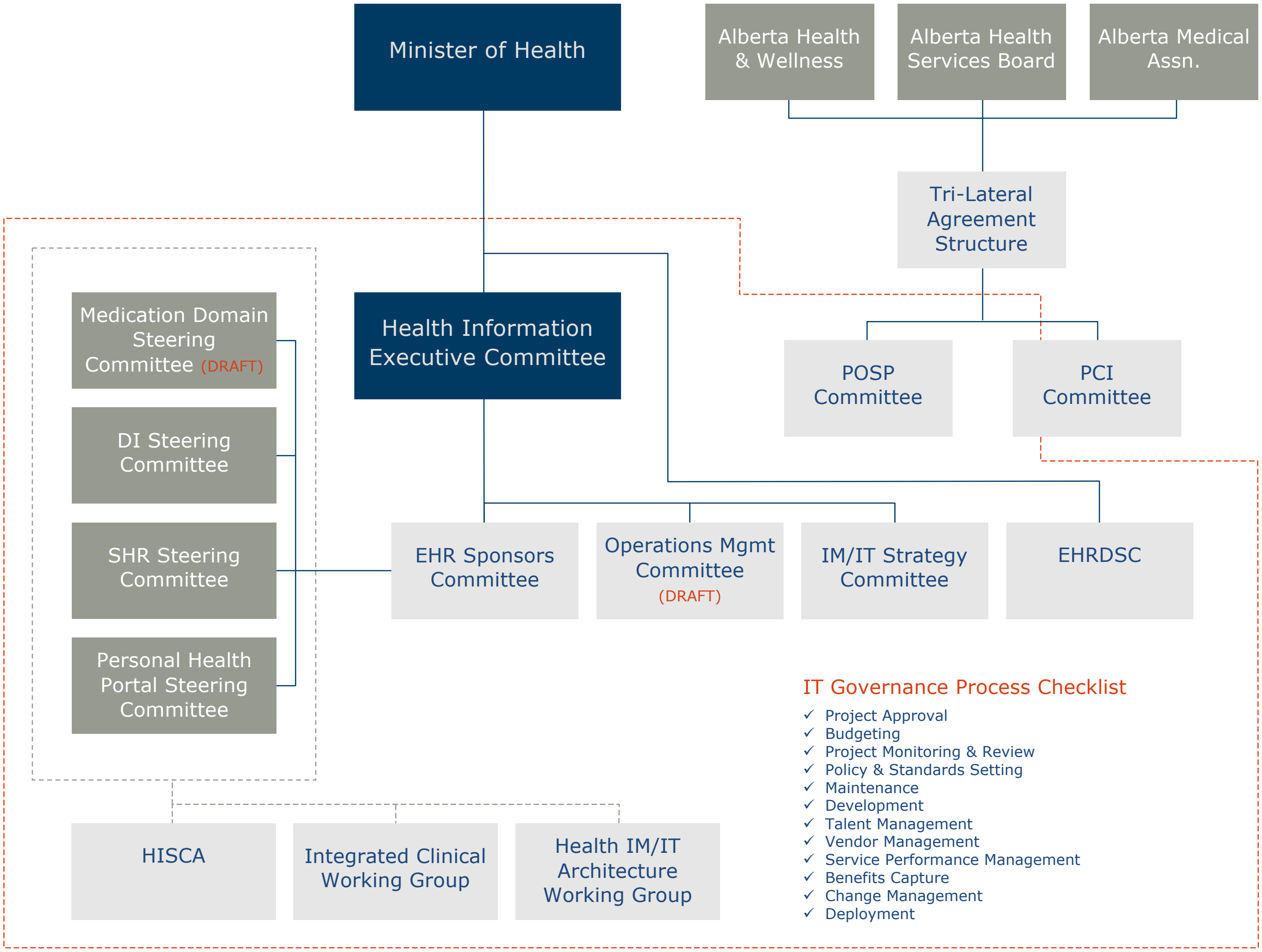
The Health Information Standards Committee (HISC-MB) provides strategic and tactical direction related to various aspects of the Information Standards Lifecycle including validating and maintaining the Enterprise Information Model, identifying and managing the health information standards policies and establishing and communicating health information standards priorities, process and procedures.

The Architecture Management Committee (AMC) is responsible for providing the architecture direction for Manitoba eHealth Provincial Projects, RHA projects, and the EHR initiative. The AMC will establish best practices, principles, and standards in the areas of application, information, security, and technology architectures through the creation and maintenance of the Enterprise Architecture (EA).

Manitoba eHealth Program Oversight Committee

The Program is supported directly by MHHL and the Manitoba Government through a separate operating funding envelope. Its overall mandate is subject to review by an Oversight Committee, reporting directly to the Minister of Health, and is chaired by the Deputy Minister. As well as the Deputy, the Committee is composed of the Deputy Minister of Science, Technology, Energy and Mines, the Chair of the Program Council as well as one member from the Council. The Committee meets twice per year to review the progress and status of the program as well as to review its plans for the future.

ALBERTA (2010)
PROVINCIAL IM/IT GOVERNANCE STRUCTURE

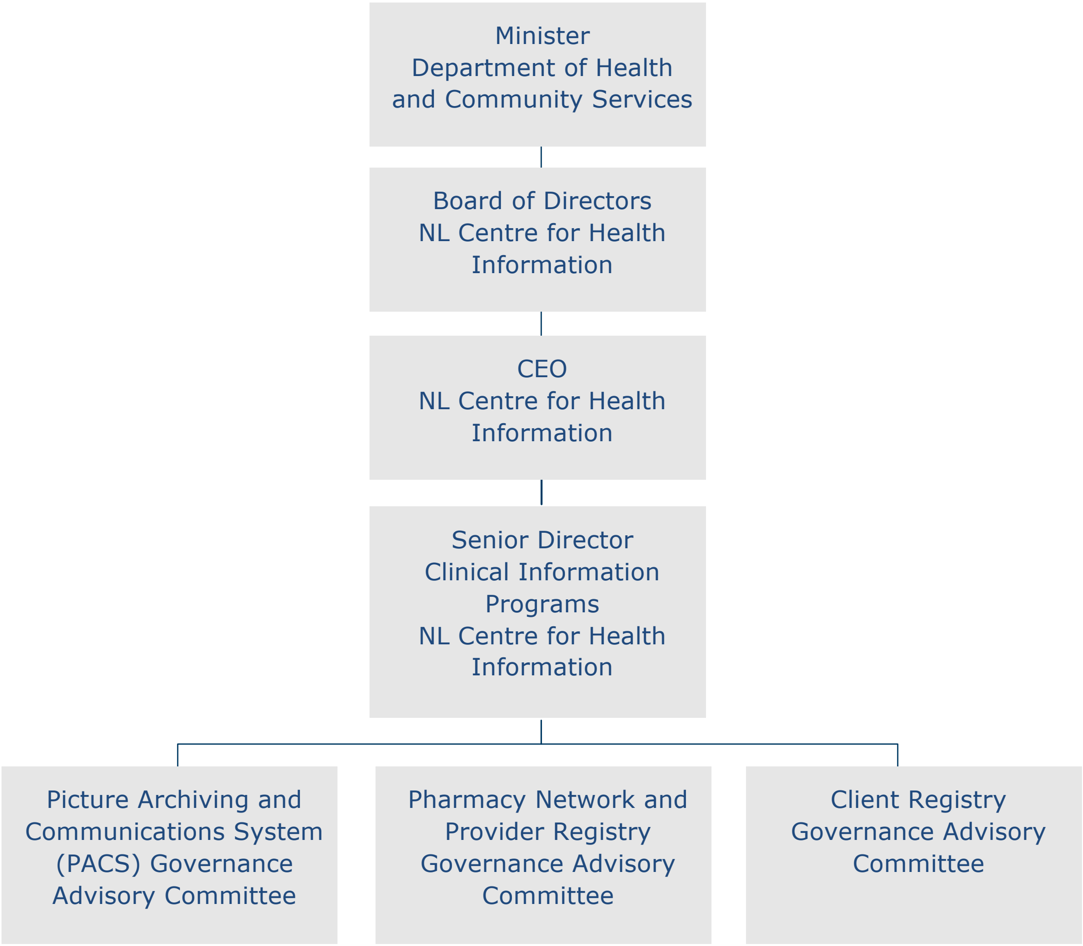

Minister of Health
Alberta Health & Wellness
Alberta Health Services Board
Alberta Medical Assn.
Tri-Lateral Agreement Structure
Medication Domain Steering Committee (DRAFT)
Health Information Executive Committee
POSP Committee
PCI Committee
DI Steering Committee
SHR Steering Committee
EHR Sponsors Committee
Operations Mgmt Committee (DRAFT)
IM/IT Strategy Committee
EHRDSC
Personal Health Portal Steering Committee
HISCA
Integrated Clinical Working Group
Health IM/IT Architecture Working Group

IT Governance Process Checklist

- ✓ Project Approval
- ✓ Budgeting
- ✓ Project Monitoring & Review
- ✓ Policy & Standards Setting
- ✓ Maintenance
- ✓ Development
- ✓ Talent Management
- ✓ Vendor Management
- ✓ Service Performance Management
- ✓ Benefits Capture
- ✓ Change Management
- ✓ Deployment

NEWFOUNDLAND AND LABRADOR EHR GOVERNANCE STRUCTURE

(AS OF JANUARY, 2010)



The Newfoundland and Labrador Centre for Health Information (the Centre) is a crown agency with a legislated mandate to assist individuals, communities, health professionals and policy makers in making informed decisions by providing a comprehensive province-wide information system. In 2007, the Department of Health and Community Services gave the Centre the mandate to govern the EHR.

The Centre is governed by a board of fifteen representatives appointed by Cabinet and reporting to the Minister of Health and Community Services. The Board of Directors represents a balance of the stakeholders in the EHR: the health system, health professionals and the community. The CEO establishes committees to advise on the strategic and operational governance of specific domains. Each committee has its own Terms of Reference and meets regularly to consider all aspects relevant to their component of the EHR. The membership of these committees represents the users of the specific domain.

Appendix C: Potential Options for the Structure and Roles of a Pan-Canadian Body for EHR Privacy and Related Information Governance

Common understandings #32 and 33 relate to the need for a single integrated pan-Canadian coordinating group to discuss, address and coordinate common privacy related information governance issues as the EHR continues to be implemented across the country. The following illustrates a range of potential structures and responsibilities for such a body that could be considered by jurisdictions as a starting point for discussions.

Committee or sub-committee of the Conference of Deputy Ministers of Health

- A pan-Canadian committee or sub-committee of the Conference of Deputy Ministers of Health (CDM) that includes a stakeholder advisory structure and makes recommendations for CDM approval. Examples of its potential responsibilities could include
  - Serving as a resource to the CDM for matters related to EHR privacy and information governance issues
  - Making recommendations towards the vision and processes for using EHR information from multiple jurisdictions for purposes other than care and treatment in a privacy-protective manner.
  - Serving as a mediator as requested, on privacy and information governance issues that are national in scope or involve more than one jurisdiction.

Pan-Canadian committee with broad, formal stakeholder representation

- A pan-Canadian committee with terms of reference, a degree of secretariat support, and broad, formal stakeholder representation (e.g., such as an advisory council linked to the committee or the inclusion on the committee of representatives from clinical, IT and other relevant domains), that provides information and updates to jurisdictions and considers jurisdictional suggestions regarding issues to explore or consider. It could, for example:
  - Contribute to national and international standards initiatives that involve or have implications for privacy and the protection of personal health information
  - Manage the creation of information materials that describe the interoperable EHR system for public information at the pan-Canadian level

New, independent organization

- A new organization established by MOU or in legislation to manage privacy and related information governance issues on behalf of jurisdictions, and to report to the Council of Ministers of Health.

Pan-Canadian Committee

- A pan-Canadian ministry committee with terms of reference and a degree of secretariat support, that meets regularly to share ideas, invite knowledge from stakeholders and consider common approaches to issues. The current HIP Group fits this category. Examples of its responsibilities could include:
    - Coordinating jurisdictional input:
        - Into privacy reviews by oversight bodies that involve more than one jurisdiction
        - To respond to questions and issues on pan-Canadian issues.
    - Maintaining and further developing pan-Canadian common understandings on privacy-related information governance matters that are national in scope or that cross jurisdictional boundaries/involve more than one jurisdiction.
    - Serving as a resource for jurisdictional EHR information governance structures.

Network of interested representatives

- An informal network of interested ministry representatives and/or representatives from jurisdictional privacy and information governance mechanisms that communicates and shares ideas and solutions on an ad hoc basis, sharing information, for example, on:
    - Emerging privacy related information governance issues
    - Relevant new technologies and tools relating to EHR privacy
    - Privacy and security breaches that involve more than one jurisdiction.

Appendix D: List of HIP Group Members 2008-2010

Joan Roch, Co-Chair (2008-2010)
Chief Privacy Strategist,
Canada Health Infoway

Lucy McDonald, Co-Chair (2008-2010)
Chief Privacy Officer/Corporate Secretary,
Newfoundland & Labrador Centre for
Health Information

Wendy Robillard , Co-Chair (from 2010)
Member from 2008-2010
Senior Manager, Information, Compliance
and Access Unit, Alberta Health & Wellness

Jurisdictional Members

Dave Morgan (from 2010)
Privacy Officer – Secondary Uses,
Newfoundland & Labrador Centre for
Health Information

Michelle MacDonald (2008-2010)
A/Manager, Privacy and Health
Information, Nova Scotia Department of
Health Health Promotion & Protection

Marina Fay (2008-2010)
Privacy & Access Coordinator / Health
Information Specialist, Corporate Services,
Prince Edward Island Department of Health

Fran White (2008-2009)
Chief Privacy Officer, Corporate Privacy
Office, New Brunswick Department
of Health

Andrea MacKenzie (2009-2010)
Senior Policy Advisor, Corporate Privacy
Office, New Brunswick Department
of Health

Sara Smallwood (from 2010)
Chief Privacy Officer, Corporate Privacy
Office, New Brunswick Department
of Health

Diane Bois (2008-2010)
Responsable et coordonnatrice des affaires
juridiques, Ministère de la santé et des
services sociaux de Québec

Carol Appathurai (2008-2009)
Director, PHIPA Review Project, Ontario
Ministry of Health and Long Term Care

Alison Blair (2009-2010)
Director, Information Management Strategy
and Policy Branch, Ontario Ministry of
Health and Long Term Care

Karen Waite (2009-2010)
Chief Privacy and Security Officer,
eHealth Ontario

Heather McLaren (2008-2010)
Chief Privacy and Risk Officer,
Manitoba e-Health

Christine E. Underwood (2008-2010)
Manager, IT/IM Privacy/Data Access Unit,
Saskatchewan Ministry of Health

Brenda Hudey (from 2010)
Health Information Solutions Centre,
Saskatchewan Ministry of Health

Deborah McGinnis (2008-2010)
A/Executive Director, eHealth Privacy
Security and Legislation Office,
British Columbia Ministry of Health

Lynda Ehrlich (2008-2010)
Senior Policy Analyst, Policy & Program
Development, Yukon Health and Social
Services

Lisa Cardinal (2008-2010)
Director, Policy, Planning & Evaluation, Northwest Territories Department of Health and Social Services

Martin Joy (from 2010)
A/Director Health Information, Nunavut Department of Health & Social Services

Philippe Tousignant (2008-2010)
Director, Access to Information & Privacy Division, Health Canada

Tina McKinnon
Director, Health Information, Nunavut Department of Health & Social Services (2008-2009);
Senior Policy Advisor, Access to Information and Privacy, Health Canada (2009-2010)

Ex officio members

Mimi Lepage
Chief Privacy Officer & General Counsel,
Canadian Institute for Health Information

Louis Barré
Vice President, Strategy, Planning and Outreach, Canadian Institute for Health Information

Canada Health Infoway

Stanley Ratajczak
Group Director, Security & Privacy Architecture

Agnes Wong
Director, Professional Practice & Clinical Informatics

Brian Foran
Privacy Specialist

Lorri MacKay
Research Specialist

Christina Northcott
Events Planner, Corporate Affairs

Jeannie O'Regan
Director, Conferences and Events

Shannon Byck
Manager, Conferences and Events

Appendix E:
List of Presentations

EHR Blueprint Version 2
http://www2.infoway-inforoute.ca/Documents/EHRS-Blueprint-v2-Exec-Overview.pdf
Ron Parker & Stanley Ratajczak, Canada Health Infoway

Electronic Health Information and Privacy Survey: What Canadians Think
http://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_EN.pdf
Mary Lysyk, Health Canada

Conceptual Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution Blueprint Version 2
http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf
Joan Roch, Canada Health Infoway

The Canadian Health Information Management Association (CHIMA)
Marci MacDonald, Halton Healthcare Services

The De-identification of Personal Health Information
Related research and presentations available at
http://www.ehealthinformation.ca/index.asp
Khaled El Emam, University of Ottawa

Panorama: The Pan Canadian Public Health Communicable Disease
Surveillance and Management Project
Krystyna Hommen, BC Ministry of Health Services

The Quebec Health Record
Diane Bois, Ministère de la santé et des services sociaux de Québec

CIO Forum
Mike Barron, Newfoundland and Labrador Centre for Health Information

Jurisdictional Scan of Patient Notices
Inventory of Health Information Governance Terminology
Jurisdictional EHR Governance Approaches
Don MacPherson, Anzen Consulting; Ross Fraser, Sextant Software

Jurisdictional Consent Models and Functionality
Ross Fraser, Sextant Software; Stanley Ratajczak, Canada Health Infoway

Infoway's iEHR Tech Project II Consent Track: Architecture and standards for Consent Directives
Ross Fraser, Sextant Software

Saskatchewan’s Patient Notification Work
Christine Underwood, Saskatchewan Ministry of Health

Health Data Warehouse and Secondary Uses:
Newfoundland and Labrador Centre for Health Information
Lucy McDonald, NLCHI; Linda Weaver & Daniel Deschênes, Emergis

Review of Selected Provincial Health Policy Centres
Michelle MacDonald & Suellen Murray, N.S. Department of Health

De-identification Process for Secondary Use
Related research and presentations available at *http://www.ehealthinformation.ca/index.asp*
Khaled El Emam, University of Ottawa

Consumer Health Solutions: *Infoway* Pre-Implementation Certification Initiative
Shelagh Maloney, Canada Health Infoway

Pan-Canadian iEHR & Privacy: Data Sharing of Personal Health Information
LCol Jim Kirkland, Federal Healthcare Partnership

Personal Health Records
Dennis Giokas, Canada Health Infoway

CIHI Health System Use Project
Louis Barre, Canadian Institute for Health Information

De-identification Tools Report
Ross Fraser, Sextant Software; Don Willison, McMaster University
http://www2.infoway-inforoute.ca/Documents/Tools_for_De-identification_EN_FINAL.pdf

Use of Data from the Electronic Health Record for Health Research
Don Willison, McMaster University

Information Sharing Agreements inventory work
Elaine Sawatsky
http://www2.infoway-inforoute.ca/Documents/ISA_report_for_HIP_Group_January_2010_EN_Final.pdf

Public Engagement Strategies
Peter MacLeod, MASS LPB

Breach Protocols in Alberta
Wendy Robillard, Alberta Health and Wellness