Canada Health Infoway
Inforoute Santé du Canada

Canada Health Infoway Inc.

White Paper on Information Governance of the Interoperable Electronic Health Record (EHR)

March 2007

Document History

Date	Description of Revision
January 2007	Original document
March 2007	Reference to the Canadian Securities Administrators (CSA) corrected on page ix. References to *Pan-Canadian Health Information Privacy and Confidentiality Framework* and the Santa Barbara County Care Data Exchange updated.

EXECUTIVE SUMMARY

Background

Infoway's mission is to foster and accelerate the development and adoption of private and secure electronic health information systems with compatible standards and communication technologies on a pan-Canadian basis with tangible benefits to Canadians. In support of this, *Infoway* has developed privacy and security requirements for an interoperable electronic health record (EHR), as well as a privacy and security conceptual architecture for an interoperable EHR infostructure.[1] As a result of this work, questions began to surface regarding who would control the data in a pan-Canadian interoperable EHR and who would be responsible for determining the personal health information[2] that end-users could access, especially when the user and the data to be accessed may be in different jurisdictions with differing privacy laws. In other words, what information governance rules would support the interoperable EHR?

This white paper is intended to contribute to understanding information governance topics in the interoperable EHR context through a discussion of:

- Current information governance topics (chapter 2);
- Canadian legal, ethical and professional requirements (chapter 3);
- Information governance structures now in use in health care (chapter 4);
- Mechanisms by which information governance is carried out (chapter 5); and
- Lessons to be learned from other countries regarding the implementation of an interoperable EHR and from other industrial sectors outside of health care that have successfully built interoperable infostructures (chapter 6).

It will be of interest to readers involved in the information governance of the interoperable EHR or one of its jurisdictional components. It will also be of interest to those who seek thorough and capable oversight of the interoperable EHR in order to maintain patient privacy and data security.

The paper has the following three objectives:

1 To describe information governance topics with privacy and security implications for personal health information in an interoperable pan-Canadian EHR;
2 To describe information governance mechanisms that are currently in use in health care in Canada and other countries, or in selected industries outside health care with lessons that could be applied to the Canadian healthcare context; and
3 To raise awareness, foster discussion, and stimulate action on important information governance topics associated with supporting a pan-Canadian interoperable EHR.

---

1 The EHR Infostructure is a collection of technical services that allow electronic health records on patients to be accessed and updated by authorized healthcare providers, regardless of where the patient and healthcare providers are geographically located within Canada. The EHR Infostructure will include access to directories of patients, healthcare provider directories, repositories of laboratory test results, diagnostic images such as X-rays, medication histories, and other essential healthcare data on patients. More information is available on *Infoway's* KnowledgeWay at http://knowledge.infoway-inforoute.ca/.

2 For the purposes of this paper, personal health information means information about the health of an identifiable individual, although more precise definitions exist in Canadian privacy legislation. References to personal information include health information which is defined as a type of personal information in Canadian public sector and private sector legislation.

Governance deals with the mechanisms that are used to guide, steer or regulate the course of an organization or system. From an interoperable EHR perspective, governance can encompass everything from corporate management of the pan-Canadian interoperable EHR to clinical issues. This paper focuses on information governance in a pan-Canadian interoperable EHR environment; i.e., those matters involved in handling personal health information in a confidential and secure manner and in compliance with appropriate legal, ethical and quality standards.

It merits noting that many of the same information governance matters are present, and have been addressed to varying degrees, in the paper health record context. However, in the interoperable EHR environment, information will flow faster, in greater volumes and potentially to more end-users. Accordingly, information governance in the EHR warrants review to ensure that the flow of information in the new EHR context is appropriately controlled.

Information Governance Topics

Chapter 2 describes a series of information governance topics with implications for the privacy and security of personal health information that would be collected, stored, and distributed in a pan-Canadian interoperable EHR. In total, there are 21 information governance topics and they are grouped as follows:

Topics related to trust and accountability include:

1. *Accountability* – This should be clearly assigned as personal health information flows through the EHR Infostructure to ensure that accountability remains clear.
2. *Openness* – Information on how data is managed and who is accountable for it should be open to public scrutiny. Patients, healthcare providers and healthcare professional bodies need to have confidence that the custodial responsibilities of healthcare providers are respected and appropriately discharged when they add personal health information into EHR repositories.
3. *Information custodianship* – In the EHR Infostructure, personal health information can flow through a complex, interconnected series of databases potentially residing in multiple jurisdictions. As the data moves, custodial responsibilities of information hosts, information contributors and information recipients need to be clear.
4. *Transborder and cross-jurisdictional data flows* – These can often be managed by data sharing agreements. A Canadian standard already exists containing guidelines on such agreements. Since the thirteen provincial and territorial jurisdictions would require multiple bilateral agreements for full interoperability, jurisdictions may want to consider other mechanisms for facilitating cross-border data flows. Questions also arise regarding the oversight powers of provincial Information and Privacy Commissioners in those cases where a complaint involves information that flowed across one or more jurisdictional boundaries. Transborder data flows to the United States raise additional issues about the potential application of the USA PATRIOT Act.

Topics related to the privacy rights of patients include:

5. *Information notices to patients* – Will the interoperable EHR require its own notices to patients regarding the collection, use and disclosure of information or can existing notices be adjusted?

6. *Information consent*[3] – The range of legal requirements regarding consent could create governance issues once personal health information in the EHR Infostructure is able to flow across jurisdictional boundaries. Technical details need to be confirmed, i.e., can a patient lock data away from specific healthcare providers? An information model for consent-related data and a consent messaging schema are needed to consistently and unambiguously represent patient consent directives.
7. *Limiting collection of personal health information* – A key privacy principle in many privacy laws is to limit the collection of information to that which is required. How will this be achieved in the interoperable EHR? For example, attention needs to be given to how the EHR will deal with data relating to family histories of disease (and hence representing information on an individual other than the record's data subject), or the potential use of free-form text fields (which do not restrict the content or scope of data input), and the ability to infer confidential information from the presence or absence of certain data values in ostensibly unrelated data fields (i.e., inferring a diagnosis from the name of a well-known specialist or specialty clinic).
8. *Limiting disclosure of personal health information and privacy-protective grouping of EHR data elements* – Law and regulations currently focus on the disclosure of health information by health information custodians and trustees. An interoperable EHR works on an access model whereby end-users pull information from the system. A shift, therefore, will occur from a disclosure-based data protection model to an access-based model where healthcare providers access the information they require to fulfill the purposes. Careful grouping of data elements could enhance privacy.
9. *Secondary use* – Over time, some EHR information may ultimately be used for secondary purposes such as public health surveillance and health system analysis and management. Some health information statutes permit such uses. However, should patients be informed of such secondary uses? What level of de-identification, is needed before personal health information that was collected for the purpose of treatment and care can be fairly and ethically used for research without requiring patient consent? Is it feasible or reasonable to expect the EHR to include information that would specifically indicate whether a patient agrees to be contacted for the purposes of health research?
10. *Patient access to data* – Three issues related to patient access are discussed: the potential ability of patients to access the entire record from a single source (the interoperable EHR), potential online access by patients, and patient challenges to the accuracy of data in EHR repositories.

Topics relating to assessment and compliance include:

11. *Risk assessment* – How can we best monitor the implementation of privacy risk mitigation strategies and integrate privacy monitoring and revisions in Privacy Impact Assessments into the EHR change management process? And what level of residual risk is acceptable?
12. *Compliance mechanisms* – Acceptable use agreements and confidentiality agreements for users of EHR systems are powerful tools for requiring compliance with

[3] Throughout this document, consent refers to patient consent to the collection, use and/or disclosure of an individual's personal health information. Consent to treatment and care is outside the scope of information governance.

privacy and security policies. Their consistent use and structure could be valuable in ensuring all users understand these agreements and are held accountable for their actions.

13. *Liability and sanctions* -- How will sanctions from multiple jurisdictions apply to an offence involving transborder data flows? Should there be specific penalties for the misuse of personal health information in a pan-Canadian interoperable EHR? Should patient identity theft be deterred by laws or regulations that explicitly protect patient directories from such exploitation?
14. *Assessment of information governance* – How will compliance with information governance policies and practices be assessed? Are some safeguards or privacy practices more cost-effective than others?

Topics related to quality in health care include:

15. *Accuracy and data quality* – Accuracy and data quality are critical in both existing personal health information systems and paper records. This is no different in an interoperable EHR environment. However, healthcare providers will need to know and understand what to expect in an interoperable EHR environment.
16. *Data retention, archiving and disposition* – Personal data should only be retained as long as is needed, but in health care, a need can arise years after the information was collected. For example, drugs taken during pregnancy may lead to neo-natal problems that do not show up in children for years or even decades. Should medication records, therefore, remain accessible online in an interoperable EHR or should they instead be electronically archived with special access being granted to the archive upon request?

Topics related to technical safeguards include:

17. *Access controls* – These are intended to prevent unauthorized access to information systems, ensure the protection of services, prevent unauthorized computer access, detect unauthorized activities and ensure information security when using mobile computing and tele-networking facilities. Technical challenges in implementing access controls that are both rigorous and easy to use are described in chapter 2.
18. *Auditing, security incident handling and privacy breaches* – Four issues related to auditing, security incident handling, and privacy breaches are identified as needing further discussion: timely handling of security incidents in the interoperable EHR, real-time auditing, preservation of digital evidence, and handling privacy breaches.
19. *Electronic (digital) signatures* – If digital signatures are allowed on prescriptions, who should issue the attendant digital certificates to users that will allow digital signing?

Finally, topics related to the rights of healthcare providers and communities of interest include:

20. *User identity management and protection of healthcare provider privacy* – Collecting personal information to identify and authenticate end-users of the system could cause concern amongst end-users if they are not given assurances that uses of the data will be limited to identity management, as opposed to the monitoring of practice patterns.
21. *Respecting communities of interest* – Discussion of privacy rights is usually focused on the rights of individuals. However, there are communities of interest, such as those related to mental health and HIV/AIDS, which also have special privacy concerns that

need to be considered when creating rules related to health information collection, use, management and disclosure. It is also now common to integrate the involvement of such groups into the governance of the relevant healthcare organizations. It will be important to consider the participation of these communities in the decision-making process. Similar questions will need to be considered regarding the involvement of Aboriginal Peoples, particularly with respect to their principles concerning ownership, access, control and possession of personal health information.

Legal, Professional and Ethical Requirements for Information Governance

Chapter 3 reviews the legislation, ethical principles and policies that currently influence the collection, use or disclosure of personal health information. It also discusses the Federal/Provincial/Territorial Advisory Committee on Information and Emerging Technologies' (ACIET) *Pan-Canadian Health Information Privacy and Confidentiality Framework*, which provides guidelines for common and consistent statutory provisions for the collection, use and disclosure of personal health information for both the public and private healthcare sectors. The protection of personal health information is influenced by: the Charter of Rights and Freedoms, federal laws such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial and territorial freedom of information and protection of privacy statutes which protect personal information in the custody or control of public or government bodies, including hospitals and regional health authorities. Alberta, British Columbia and Quebec have private sector privacy legislation that protects personal information, including health information held by private health sector entities, including pharmacies, laboratories and private clinics. Quebec also protects personal health records held by public and private health and social service institutions. As well, there are four provinces that have enacted legislation specific to health information that contains specific rules relevant to electronic health records. Relevant examples are cited from each of the above.

Physicians and other healthcare providers are bound by additional statues. For example, in Ontario, physicians are bound by the *Medicine Act* and nurses are bound by the *Nursing Act*. Public hospitals in Ontario are bound by the *Public Hospitals Act.* Other jurisdictions have similar legal requirements beyond what is specified in privacy statutes. Legislation may also establish a healthcare organization or facility, but leave the details of a privacy and security regime to regulations that must also be taken into consideration.

While Canadian privacy laws are lengthy and complex, most are based on internationally accepted fair information principles which form the basis for the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). The principles tend to work well when applied to information held within a single organization, but may be more difficult to apply to an interoperable EHR. Several practical examples are given of the challenges presented in applying the 10 principles to the operation of the EHR.

Codes of professional conduct must also be taken into account in arriving at effective information governance. National health professional associations have produced general codes of ethics, privacy guidelines and other resources to guide their members on issues of confidentiality and health information management. Other organizations, such as provincial regulatory health colleges and research ethics boards, have also created privacy and security guidelines for use in health care and when dealing with personal health information.

Privacy laws also empower Information and Privacy Commissioners with oversight to ensure compliance with the law. They are charged with the responsibility of overseeing information practices subject to legislation, which also includes privacy protective information practices for EHR implementations.

The laws, regulations, and codes of conduct described above all have implications for information governance of the interoperable EHR.

Information Governance Structures in Canadian Health Care

Information governance is already being carried out among health information custodians, trustees and institutions that administer health care in Canada. Chapter 4 describes how some healthcare organizations have addressed information governance:

- In primary care practices (Alberta's Physician Office System Program is discussed as an example in section 4.2);
- In healthcare institutions such as hospitals (*University Health Network* in Toronto is discussed as an example in section 4.3),
- In regional health authorities (*Vancouver Coastal Health* is described as an example in section 4.4),
- In government-funded agencies that deal with a specific disease, such as cancer, mental health, or HIV/AIDS (*Cancer Care Ontario* is discussed as an example in section 4.5);
- In provincial information infostructures (the *Newfoundland and Labrador Centre for Health Information,* the Ontario *Smart Systems for Health Agency,* and the Alberta *Data Stewardship Committee* are all discussed as examples in section 4.6); and
- In healthcare organizations with large public holdings of personal health information (BC *Pharmanet* is discussed as an example in section 4.7).

Information Governance Mechanisms in Canadian Health Care

Chapter 5 describes information governance mechanisms that are currently in use in the Canadian healthcare system. These mechanisms include:

- *Statement of Information Practices* – By means of brochures, posters, notices posted on walls and websites, and verbal explanations, many healthcare providers and organizations already provide their patients with a statement of information practices.
- *Privacy policy* -- Many healthcare organizations already have a written privacy policy, sometimes based upon the CSA Model Code.
- *Security policy* -- Security policies are an important part of the security component of information governance.
- *Other policies related to information governance* – These include a system access policy; a policy on access to personal health information for research, education and quality assurance purposes; a policy to address requests to access and correct personal health information in patient records; and a policy on retention and destruction of health records.

- *Privacy officers and privacy teams* – Individuals are to be designated to interpret the requirements of applicable legislation, provide ongoing privacy training and answer questions about data protection and security from patients; as well as manage crises as real problems arise.

- *Information security officers and security teams* – Working closely with Privacy Officers, individuals responsible for information security management and information security technology are also instrumental in handling information governance management.

- *Privacy and security awareness training* – Breaches of privacy are often related to failures in information security that can, in turn, be traced to users who did not understand, or did not follow, established security-related procedures. The importance of training in the electronic health record environment cannot be underestimated with regard to ensuring that all users of the system understand the power of the EHR systems, authorized uses of the system and the penalties for misuse.

- *Memoranda of understanding, confidentiality agreements, acceptable use agreements, data-sharing agreements* – These can all be valuable tools to help ensure that partners and users of the EHR are aware of: their respective obligations on a variety of matters, including the need to meet legal requirements for data protection and security and the importance of complying with the terms of use of electronic systems and in keeping information confidential. Data-sharing agreements are a privacy best practice and can include privacy protective clauses related to restrictions on agents, general limitations, notification requirements, privacy requirements, inspection, audit and enforcement clauses, and liability and sanctions to ensure end-users accept responsibility for maintaining the confidentiality of personal information obtained from EHR systems.

- *Monitoring compliance* – Real-time auditing and other technical and administrative measures can be implemented to minimize privacy breaches by monitoring access to and use of EHR systems.

- *Security audit mechanisms* – Security vulnerability assessments are often carried out on large, operational IT systems to evaluate their security status. Penetration testing is also sometimes performed by a qualified third party on operational systems.

Lessons Learned from Other Jurisdictions and Other Industrial Sectors

Chapter 6 describes work done on information governance in the UK, Australia and the US. In the UK, the Department of Health has been grappling with information governance issues since 2001. The UK *National Health Service (NHS) Information Governance Toolkit* measures the state of information governance in British hospitals. The toolkit's questions are divided into a number of categories, such as healthcare records management, clinical information assurance, confidentiality and data protection assurance, secondary uses, and information security assurance. While the approach involves self-assessment, a written statement must accompany each answer, stating what evidence is available to support the answer given. The results of the assessment are carefully reviewed and hospitals are rated on their responses. After several years of use and refinement, hospitals now work hard to improve below-average scores and aspects of the assessment are made available to interested members of the public.

Because of the many Canadian stakeholders and jurisdictions that would be involved in an interoperable EHR, cooperation will be an important factor in the success of information governance for the interoperable EHR. Cooperative ventures have succeeded in other countries and the paper briefly examines one such endeavour: the Santa Barbara County Care Data Exchange. Several information governance lessons were learned over the years in which the Exchange has developed and grown. For example, physician concerns were raised about whether the clinical data exchanged could be pooled and used to profile or evaluate their practices and assurances needed to be put in place that this would not happen. There was also user resistance to security certificates and requests for other forms of authentication.

Scale, scope and complexity need not be barriers to effective EHR deployment. Kaiser Permanente is the largest non-profit health plan in the United States, serving the healthcare needs of 8.2 million patients. As of 2003, Kaiser had 135,000 employees and 11,000 physicians. The Kaiser Permanente HealthConnect program is currently the world's largest deployment of an EHR. It integrates clinical records with appointments, registration and billing: a patient's medical history is available to every clinician who is involved in that patient's care. It includes features such as maintenance of a patient medication profile, drug interactivity checking, online access by patients to portions of their record, and online appointments booking. Security features include role-based access control. Indeed, the size, scope and sophistication of Kaiser's EHR mirror many aspects of the interoperable EHR envisioned by *Infoway*. The system is described in section 6.1.

There are also lessons to be learned from other industrial sectors that have built large-scale and complex information infrastructures and these are described in section 6.2. Interac develops and operates Canada’s national network of two shared electronic financial services: cash dispensing at Canada's 35,000 automated banking machines (ABMs) and Interac Direct Payment, responsible for transacting two billion online purchases. The Interac experience shows that a large scale, Canada-wide IT network can be efficiently deployed and governed to enable highly reliable, high-volume exchanges of confidential personal information among a diverse set of stakeholders.

The Canadian Securities Administrators (CSA) is a forum for the 13 securities regulatory authorities of Canada's provinces and territories to coordinate and harmonize regulation of Canadian capital markets. Despite jurisdictional variances in securities legislation and regulations, the CSA has determined a core set of regulatory requirements that are substantially the same in all jurisdictions. The CSA works toward regulatory initiatives that are coordinated across the country, as its members believe these best serve investors and markets. CSA members also believe regulation must accommodate both national and local concerns, priorities and issues. Those readers concerned about the effect inter-jurisdictional data transfers may have on health information custodial responsibilities may find the CSA's approach of interest.

Australia has produced a standard on information governance. It provides a framework of principles for boards of organizations to use when evaluating, directing, and monitoring the IT portfolio of the organization. The standard lays out six principles for good information governance related to establishing clearly understood responsibilities, planning, acquisition, performance, conformance and respect for human factors. It also provides a model that directors of organizations can follow when evaluating the use of IT, preparing and implementing plans and policies, and monitoring conformance to policies. A framework is included that guides implementers of the standard on how best to implement each of the six principles. This standard is related to another Australian standard that provides guidance on good governance principles and codes of conduct. This second standard on corporate governance (not specifically related to IT) discusses structural elements of good governance and lays out governing board responsibilities, disclosure and transparency obligations, and the roles of stakeholders in governance. While no similar Canadian standards exist yet, these Australian standards are a good starting point for the elucidation of information governance principles.

The International Air Transport Association (IATA) is the primary vehicle for inter-airline cooperation in promoting safe, reliable, secure and economical air services among the 270 airlines that make up its membership. The safety and security of airlines systems are no less critical than those in health care and IATA has surmounted legal, regulatory, operational and practical barriers to promote the smooth interoperation of sophisticated mission-critical IT systems that span 140 countries. This was achieved cooperatively in spite of IATA's members being business rivals in the highly competitive airline industry.

Conclusions

The overall objectives of the pan-Canadian interoperable EHR initiative are to increase the efficiency of the health system, improve access to health services and improve the quality of health service provided to Canadians. This will be achieved, in part, by increasing the speed and volume of information being shared or transferred amongst authorized end-users.

Governance is not a new concept and information governance is not new to the health record environment. Many components of information governance discussed in this paper apply and have been addressed in varying degrees in the paper world of health records. However, the interoperable EHR changes the environment within which information will flow. As such, the rules related to information collection, use, disclosure and management in an interoperable EHR environment bear careful review, especially if EHR initiatives are to be accepted by healthcare providers and the public.

With respect to the vast array of information governance topics identified in this paper, the large number of diverse stakeholders with interest in these topics and the complex legislative, regulatory and ethical schema that must be taken into account, it is likely that a variety of approaches to information governance will be required. These options could involve cross-disciplinary committees, or intra-jurisdictional working groups or teams, among others, to identify and arrive at information governance solutions for a pan-Canadian interoperable EHR.

Consideration also needs to be given as to where responsibility for information governance management will reside. Perhaps it can be managed from within existing information governance structures, or perhaps, similar to Interac, the Canadian Securities Administrators and the International Air Transport Association, an additional central structure will be necessary in order to be seen to provide an effective and efficient way to manage some of the information governance topics identified in this paper.

Information governance in the interoperable EHR is already beginning to be addressed and considered by many involved in the EHR initiative. It is recognized that it will take time to involve the necessary stakeholders and arrive at acceptable approaches. Currently, EHR developments are primarily domain- and jurisdiction-based and it will be some time before interoperability is achieved within a jurisdiction, let alone at a pan-Canadian level. As such, while some topics, such as role-based access, may require attention in the short term, in other cases there is time to address the topics in an incremental manner, over time, on an intra-jurisdictional basis as the components of interoperable EHR systems develop and as the information necessary to arrive at reasonable approaches becomes available. Further, as noted in the paper, there are many information governance mechanisms currently in place that apply to the world of paper-based records, which can be leveraged for the development of future information governance solutions in a pan-Canadian interoperable EHR environment.

This paper is intended to foster discussion and promote action. Readers are encouraged to share this paper with their colleagues.

Infoway also remains committed to exploring these topics and to this end will be meeting with stakeholders during the winter of 2007. Comments can also be submitted directly to:

Joan Roch, Chief Privacy Strategist
Canada Health Infoway
1000 Sherbrooke Street West, Suite 1200
Montreal, Quebec H3A 3G4

Tel: (514) 237-0521
Fax: (514) 221-2258
Email: jroch@infoway-inforoute.ca

Canada Health Infoway Inforoute Santé du Canada

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

At their meeting on health in September 2000, the First Ministers agreed to collaborate on strengthening a Canada-wide health infostructure to support improvements to the quality, accessibility and timeliness of health care for Canadians. As a result of this meeting, the federal, provincial and territorial governments formed Canada Health Infoway. The Deputy Ministers of Health of the various jurisdictions serve as *Infoway's* members.

Infoway's mission is to foster and accelerate the development and adoption of private and secure electronic health information systems with compatible standards and communication technologies on a pan-Canadian basis with tangible benefits to Canadians. *Infoway's* vision is of a high-quality, sustainable and effective Canadian healthcare system supported by an infostructure that provides residents of Canada and their healthcare providers with timely, appropriate and secure access to the right information, when and where they enter the healthcare system. Privacy is fundamental to this vision in support of *Infoway's* goal of improved productivity, access and quality in the delivery of healthcare services to Canadians through an interoperable electronic health record (EHR).[4]

In support of its vision, *Infoway* has developed privacy and security requirements for an interoperable EHR, as well as a privacy and security conceptual architecture for an interoperable EHR. These documents are available on *Infoway's* KnowledgeWay at http://knowledge.infoway-inforoute.ca/. During development of these documents, questions began to arise, such as, who controls and has custody of the data in a pan-Canadian interoperable EHR? Who is responsible for determining the extent of personal health information that end-users may access? Who resolves complaints about the handling in one jurisdiction of personal health information obtained from another? What are the permissible secondary uses of personal health information from a pan-Canadian interoperable EHR? In other words, what information governance rules support the flows of personal health information that may be involved in the EHR vision and who is ultimately accountable for ensuring compliance with these rules?

This paper is intended as a reference document that will contribute to understanding of the above information governance questions by providing the reader with a discussion of:

- Information governance topics (chapter 2);
- Canadian legal, ethical and professional requirements (chapter 3);
- Information governance structures currently in use in health care (chapter 4);
- Mechanisms by which information governance is currently carried out (chapter 5); and
- Lessons from other countries and sectors outside of health care that have successfully built interoperable infostructures (chapter 6).

Achieving meaningful data protection is an ongoing process, requiring organizational and individual commitment, as well as the allocation of resources for monitoring and for education about privacy rules for all of those involved in health care, including patients and their families. The goal is to achieve a balance among the needs of patients, the effective delivery of health

[4] http://www.infoway-inforoute.ca/en/WhoWeAre/Overview.aspx

care and the protection of the human right to personal privacy as articulated in the Canadian Charter of Rights and Freedoms.

Senator Michael Kirby has underscored the critical need "to improve the governance of Canada's healthcare system,"[5] stressing that the "underlying issue is one of accountability"[6]. The interoperable EHR is one part of the health system. Its governance similarly requires attention to ensure clear accountability, effective functioning and the adequate protection of the personal health information it will hold.

1.2 White Paper Objectives

As health information is increasingly collected, stored and disclosed in electronic form, there is growing awareness and sensitivity about who is responsible for protecting patients' privacy and security. *Infoway* recognizes that privacy and security are an integral part of what Canadians consider quality health care. *Infoway* also recognizes that Canadians should be able to have as much confidence in an interoperable EHR as they do in the electronic services of the Canadian banking system.[7] In order to achieve this, it is important to identify common rules that all users of the system will follow.

In recognition of this, the paper has the following three objectives:

1. To describe information governance topics with privacy and security implications for personal health information in an interoperable pan-Canadian EHR;
2. To describe information governance mechanisms that are currently in use in health care in Canada and other countries, or in selected industries outside health care, with lessons that could be applied to the Canadian healthcare context; and
3. To raise awareness, foster discussion, and stimulate action on important information governance topics associated with supporting a pan-Canadian interoperable EHR.

1.3 Who Should Read This White Paper?

This paper is intended as a reference document for readers who are, or will be, involved in the information governance of the interoperable EHR or one of its jurisdictional components. It will also be of interest to those who want thorough and capable oversight of the interoperable EHR in order to maintain patient privacy and data security.

The paper presumes some familiarity with the general precepts of information governance, as well as a familiarity with the purpose and overall features and benefits of the interoperable EHR. Readers who lack this familiarity may find the following references useful:

---

5 "Improving Governance – the Need for a National Health Care Commissioner". *The Standing Senate Committee on Social Affairs, Science and Technology. Michael J.L. Kirby (Chair). The Health of Canadians: the Federal Role. Final Report. Volume Six: Recommendations for Reform.* Ottawa: The Senate, 2002. Chapter 1, Section 1.2.

6 Ibid.

7 The Interac Association is described in section 6.2.

- A good background on the governance of Canadian non-profit organizations can be found at the Canadian-based Institute for Good Governance (http://www.iog.ca/). For example, the *Institute's* paper, *Governance Do's and Don'ts: Lessons from Case Studies on Twenty Canadian Non-Profits,* describes how good governance is achieved in the Canadian not-for-profit sector. The paper is available at http://www.iog.ca/publications/nonprofit-gov.PDF.

- A general discussion of information governance can be found at the US-based IT Governance Institute (http://www.itgi.org). The Institute has produced two good background papers: *Board Briefing on IT Governance,* available at http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=4667
and "*IT Governance Executive Summary"*, available at
http://www.itgi.org/ContentManagement/ContentDisplay.cfm?ContentID=19976

- The reader looking for fundamental principles underlying information governance will find the document "*Good Governance Principles"* from Standards Australia. It can be purchased online from http://www.saiglobal.com

- A description of the interoperable EHR can be found in the *Infoway* infosheet available at http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Infosheet_E_IEHR_Final.pdf

- In 2005, *Infoway* produced an analysis of privacy and security principles that should be upheld by the interoperable EHR. They can be found in *Electronic Health Record (EHR) Privacy and Security Requirements, version 1.1, 2005* available at http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Requirements.pdf

- The Federal/Provincial/Territorial Advisory Committee on Information and Emerging Technologies ("ACIET") released its *Pan-Canadian Health Information Privacy and Confidentiality Framework* ("ACIET Framework") in 2005; the ACIET Framework is available at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html#intro.

1.4 Scope

Governance can encompass everything from the financial management of an interoperable EHR to clinical issues for healthcare providers who need to access, interpret and use EHR information properly. This paper focuses on information governance. It discusses the rules, requirements (legal, ethical and practical) and mechanisms that are involved in handling personal health information that would be collected and used in a pan-Canadian interoperable EHR in a secure and privacy-protective manner.

Financial governance and clinical governance are outside the scope of this discussion. The authors acknowledge that questions about information governance may have important intersections with clinical governance matters. For example, if a personal health information domain repository failed to maintain the integrity of a patient's medication history or lab test results during transmission or storage, there could be liability issues if healthcare providers made incorrect diagnoses or provided inadequate care on the basis of that faulty information.

The medico-legal issues related to such governance issues are important to the successful adoption of the interoperable her, but they are outside the scope of this paper.

2. INFORMATION GOVERNANCE TOPICS WITH PRIVACY AND SECURITY IMPLICATIONS FOR PERSONAL HEALTH INFORMATION

2.1 Introduction

This chapter outlines information governance topics associated with the management of personal health information in an interoperable EHR. They include issues relating to the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information,[8] as well as issues that arise from Canadian privacy legislation and from practical or ethical challenges associated with custodianship or trusteeship,[9] transborder and cross-jurisdictional data flows, incident handling and security safeguards that are a part of *Infoway's* Privacy and Security Conceptual Architecture.

In total, 21 information governance topics are discussed, grouped as follows:

Topics related to trust and accountability (see section 2.2)

1 Accountability and trust

2 Openness

3 Information custodianship

4 Trans-border and cross-jurisdictional data flows

Topics relating specifically to the privacy rights of patients (see section 2.3)

5 Information notices to patients

6 Information consent

7 Limiting collection of personal health information

8 Limiting disclosure of personal health information and privacy-protective grouping of EHR data elements

9 Secondary uses

10 Patient access to data

Topics related to assessment and compliance (see section 2.4)

11 Risk assessments and privacy impact assessments

---

8 CAN/CSA-Q830-96 was designed as a voluntary code for privacy protection among private sector organizations. It was published in March 1996 and was adopted as the national standard for privacy protection in Canada. It has also been incorporated as Schedule 1 of the federal *Personal Information Protection and Electronic Documents Act, 2001*. These core principles facilitate an easily recognisable, principled approach to data protection.

9 For the purposes of this white paper, we will use the phrase "health information custodians and trustees" to refer to any entity assuming custodial responsibility for health information in its possession. The phrase "health information custodians and trustees" is intended to include the following types of organizations in possession of health information: a "custodian" under Alberta's *Health Information Act*, a "health information custodian" under Ontario's *Personal Health Information Protection Act, 2004*, a "trustee" under Manitoba's *Personal Health Information Act* and Saskatchewan's *Health Information Protection Act*, a "public body" under public sector legislation across Canada including Quebec, an "organization" under the *Personal Information Protection Act* in Alberta and British Columbia, and a "private enterprise" under Quebec's private sector legislation.

12 Compliance mechanisms

13 Liability and sanctions

14 Assessment of information governance

Topics related to quality in health care (see section 2.5)

15 Accuracy and data quality

16 Data retention, archiving and disposition

Topics related to technical safeguards (see section 2.6)

17 Access controls

18 Auditing, security incident handling and privacy breaches

19 Electronic (digital) signatures

Topics related to the rights of healthcare providers and communities of interest (section 2.7)

20 User identity management and protection of healthcare provider privacy

21 Respecting communities of interest

This list is neither exhaustive nor prescriptive. Rather, the list reflects information governance topics the authors were able to identify and describe at the time of writing this paper.

2.2 Topics Related to Trust and Accountability

1 Accountability

The first principle of the CSA Model Code, accountability, is currently reflected in many privacy statutes in Canada. It requires organizations that collect, use or disclose[10] personal information to clearly identify individual(s) responsible for ensuring compliance with applicable data protection legislation and institutional privacy policies. It already applies to existing paper systems, but needs to be revisited in the interoperable EHR context.

Personal health information is already disclosed in the paper system by one healthcare provider to another and from one healthcare organization (e.g., a clinic or hospital) to another. However, in the interoperable EHR context, this will increase and chains of accountability may become complex. Each stakeholder in the process has certain legitimate expectations. Patients look to their healthcare providers to protect the confidentiality of their personal health information. Providers disclosing data to healthcare institutions, such as hospitals, rely on the due diligence of these institutions. Institutions, in turn, may rely upon a provincial health network to safeguard personal health information in transit and storage. Providers also rely upon their professional associations and provincial regulatory colleges for guidance on standards of practice in the handling of personal health information. Finally, the public relies on federal, provincial and territorial governments to protect public interests by enacting privacy protective laws and regulations and by ensuring independent oversight, such as that provided by provincial and

[10] Use refers to any processing and treatment of data within an organization, whereas disclosure refers to the release of the information to third parties (outside of the originating organization, even in an EHR environment).

territorial Information and Privacy Commissioners. To be effective, accountability for personal health information needs to be clearly assigned throughout the EHR Infostructure.

This may mean that contracts and agreements that are in effect among healthcare providers, institutions and IT service providers may need to be reviewed and enhanced to ensure accountabilities and EHR responsibilities in the new environment are appropriately reflected. In the future, where information flows from one region to another or across provincial borders for processing, as well as for care and treatment purposes, broader and more comprehensive contractual agreements than those existing today will likely be needed with vendors and service providers to ensure that accountability is maintained. Responsibility cannot be outsourced. Each participating individual and institution needs to fulfill its data protection responsibility in order for the chain of accountability to remain intact.

2 Openness

The information in the EHR Infostructure must not only be effectively governed; it must be seen to be effectively governed. Openness is another principle within the CSA Model Code. Transparency in governance structures and governance processes is paramount if the trust of patients and the public is to be maintained.

Canadians have historically been uncomfortable with the notion of placing large databases of identifiable personal information under the direct care of federal, provincial or territorial governments. In response, several provincial governments have set up agencies to handle the networking, administration and safekeeping of such EHR databases. The governance of these agencies is at least partially at arms-length from government.[11] These agencies also require openness and transparency in their dealings with patient privacy.

Patients will look both to their healthcare providers and to provincial or territorial governments to ensure that their personal health information remains confidential wherever it is held or however it is transferred between custodians and EHR databases, within or across jurisdictions. Information on how the data is being managed and who is accountable in every instance should be open to public scrutiny.

3 Information Custodianship

The responsibilities of health information custodians and trustees are defined in health information legislation. As data moves among healthcare custodians and trustees, each custodian must trust that the others are upholding these responsibilities.

Even though custodians and their obligations are often defined in statutes, data custodianship or trusteeship is still a controversial issue in electronic health record environments. For example, at the annual Canadian Medical Association (CMA) meeting, held in 2005, an important resolution identified by delegates and put forth to the CMA Board of Directors called for the CMA to ensure physicians remain the custodians of physician-generated health information in the primary care setting. This motion reinforced recent CMA initiatives to raise awareness about data stewardship in the face of concerns about the development of large data repositories.[12] Furthermore, although it may be discerned from the statutes as to who the

[11] The Saskatchewan Health Information Network and the Ontario Smart Systems for Health Agency are two examples of such arms-length agencies.

[12] See "*Information Technology was a Top-of-Mind Issue for Delegates Attending the CMA Annual Meeting in Edmonton Last Week*" at http://www.cma.ca/index.cfm/ci_id/45344/la_id/1.htm

custodian is in a single organization or for a single domain repository, the custodianship of the shared health record remains unclear.

In the EHR environment, personal health information could flow through many interconnected series of databases and over time could reside in multiple jurisdictions. As data moves from one custodian to another custodial responsibilities move with it. Custodial responsibilities can include ensuring consent is appropriately obtained and consent directives honoured before data is disclosed; providing access only to authorized users; ensuring data is used only for the purposes intended when it was collected; proper safeguarding of the information; and ensuring that the supporting information systems maintain the data's confidentiality and integrity. The clear identification of custodial responsibilities will be a primary information governance challenge for the interoperable EHR.

Infoway's Privacy and Security Conceptual Architecture is built on the dual assumption that every implementation of the EHR Infostructure will store personal health information under the governance of the implementing jurisdiction(s) and that the consent provisions of the disclosing jurisdiction will be upheld by a recipient jurisdiction before the information is disclosed. It is not yet clear what information handling processes would be needed in recipient jurisdictions to honour the disclosing jurisdiction’s privacy and security requirements.

4 Transborder and Cross-Jurisdictional Data Flows

Transborder flows of data can be managed by data-sharing agreements among jurisdictions. An example of a list of minimum criteria for legal and contractual agreements can be found in CSA standard CAN/CSA-Z22857-06 (ISO 22857:2004) *Health informatics — Guidelines on data protection to facilitate transborder flows of personal health information*. This Canadian and international standard[13] contains principles that should be upheld when personal health information flows across international borders and also contains exemplary contract clauses that can be used as models in the construction of data-sharing agreements. While the discussion is primarily aimed at international borders, most of the principles and exemplar contract clauses are applicable to intra- and interprovincial and territorial data flow as well. Such existing work can be used as a basis for discussions about the minimum criteria needed for cross-jurisdictional agreements, although much more work also needs to be done.

It is worth noting that the 13 provincial and territorial jurisdictions would require multiple bilateral agreements for full interoperability. Thought should be given as to whether negotiating a series of bilateral agreements for each jurisdiction is the most appropriate approach to facilitating cross-border data flows or if another approach would be more effective.

Questions may also arise regarding jurisdictional exercise of the oversight powers of provincial Information and Privacy Commissioners in those cases where a complaint involves information that flows across one or more jurisdictional boundaries. One of the purported advantages of the EHR Infostructure is that personal health information will be readily available on a patient who is travelling away from home. Personal health information is held where it is captured, not where the person lives. It is not difficult, therefore, to imagine personal health information being collected in one jurisdiction on a patient residing in a second jurisdiction and a privacy breach occurring after a disclosure (to a specialist, for example,) in a third jurisdiction. In an attempt to

[13] The Canadian standard (CAN/CSA-Z22857-06) contains additional text that deals explicitly with such issues as the rights of data subjects to pursue an objective investigation, by an appropriate authority in the data subject's jurisdiction. It also explicitly references the role of provincial/territorial privacy commissioners.

resolve these issues, Information and Privacy Commissioners are increasingly working together to investigate non-health-related complaints that involve multiple jurisdictions. [14] It remains to be seen how specific problems arising from inter-jurisdictional data flows in the interoperable EHR will be addressed.

Transborder data flows to the United States raise additional issues. Questions about the potential application of the USA PATRIOT Act continue to concern health information custodians and trustees and at least one jurisdiction, British Columbia, has reacted decisively to counter this perceived challenge to individual privacy and responsible custodianship. [15] Section 215 of this Act permits the Federal Bureau of Investigation to seek access to personal information using a secret warrant in pursuit of international terrorism investigations. This gives US law enforcement authorities power to gain access to Canadian personal information in records held by a US-linked firm, including a Canadian company operating in the US. Therefore, effectively ensuring that data in the interoperable EHR remains under Canadian jurisdictional control warrants special attention when negotiating contracts with EHR service providers.[16]

2.3 Topics Related to the Privacy Rights of Patients

5 Information Notices to Patients

The CSA Model Code and many privacy statutes in Canada state that patients are to be informed of the purposes for which custodians and trustees collect, use and disclose personal health information and of the safeguards that are in place to protect it, in a readily understandable manner, at or before the time information is collected. This notice requirement may be fulfilled through posters, brochures or websites where patients may obtain information on their healthcare provider’s information practices. This requirement exists in many jurisdictions today in the paper world.

---

[14] See reports on the joint investigation conducted by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of Alberta into misdirected faxes containing personal health information and the alleged contravention of both the Federal *Personal Information Protection and Electronic Documents Act* and the Alberta *Health Information Act*, which the Commissioners oversee, respectively, available at: (Federal report) http://www.privcom.gc.ca/media/nr-c/2004/ab_041221_e.asp and (Alberta report) http://www.oipc.ab.ca/ims/client/upload/H2004-IR-001.pdf.

[15] Information and Privacy Commissioner of British Columbia “*Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing*", October 2004; available at: http://www.oipcbc.org/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf

[16] This issue was recently addressed in an independent investigation conducted by the Ontario Information and Privacy Commissioner concerning a contract between Cancer Care Ontario (CCO) and the US vendor selected to implement the provincial Electronic Master Person Index. In her review, the Commissioner found that CCO had adequate written privacy, confidentiality and security provisions in its Master Software License and Services Agreement with the vendor to address the issue. For example, the agreement included a prohibition on disclosures to third parties outside Ontario without prior written consent of CCO or unless requested by a Canadian court or other Canadian authority with jurisdiction to compel disclosure. The agreement also required all personal health information to be maintained and stored in Ontario. Nor was the vendor permitted remote access to the data. See Information and Privacy Commissioner’s News Release “*Electronic health information strongly protected in Ontario: Commissioner Cavoukian*,” at: http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=17105&U_ID=0

Where such information is provided to the public, it is typically in relation to a specific domain repository initiative, such as a pharmacy network or a hospital or primary care physician's office. Consideration needs to be given as to whether existing notices are sufficient to cover the interoperable EHR, if existing notices can be adjusted or if the EHR warrants a separate notice.

6 Information Consent

Provincial/territorial privacy laws may require express, implied, deemed or no consent for specific collections, uses and disclosures of personal health information. The range of legal requirements regarding consent could create governance issues once personal health information in the EHR Infostructure is able to flow across jurisdictional boundaries. Three issues in particular need further discussion and resolution; they are outlined below.

Information Model for Consent-Related Data and a Consent Messaging Schema

Infoway's Privacy Requirement 10 states that the EHR Infostructure must be able to record a patient's consent directives, including the withholding, withdrawal or revocation of consent, and furthermore, that it should be able to do this in a way that allows each jurisdiction to comply with its own legal requirements on consent. Related are Privacy Requirements 13 and 15, which deal with logging the application of consent overrides and the recording of the identity of substitute decision-makers. A formal information model has not yet been developed for capturing data fields that identify the type of consent obtained (i.e., express, implied, etc.), the time it was obtained, and the person from whom it was obtained (from the patient or from a substitute decision-maker for example), nor for the parallel information that must be collected in cases of withdrawal or revocation of consent. The model must be flexible and robust enough to allow implementations tailored to each jurisdiction's requirements, while simultaneously supporting intra- and inter-jurisdictional data flows.

Consent directives also need to be transmitted with data whether the data is disclosed intra- or extra-jurisdictionally. Thus, a messaging schema will be needed that supports the information model for consent directives and allows consent data to be transmitted along with the data disclosed. Messaging schema are now being addressed in a new Infoway project on iEHR Technical Standards.

Overriding Consent in Emergencies

As a practical matter, consent provisions may need to be overridden during medical emergencies. In keeping with the public's concern that only authorized individuals have access to their information, it is important that the identity of any user who overrides a patient/person's consent directives be logged, along with the reason for the consent override, and the date and time when the consent override occurred. It also important that the individual accountable for privacy compliance in the organization where the accessing user works, and the organization from which the information was collected, be alerted whenever such a consent override occurs. The practical details of how this should be implemented effectively need to be considered as data begins to flow between custodians, data domain repositories and across jurisdictional boundaries.

Locking Data

The ability of a patient to expressly withhold or withdraw consent to the disclosure of a portion of his or her personal health information for healthcare purposes, except during a medical emergency, is often referred to as "locking" data[17]. The concept of a "lock box" where especially sensitive personal health information can be placed is not yet uniformly understood in operational terms, even in jurisdictions where privacy legislation expressly requires such a construct[18]. In implementing this feature, thought needs to be given to what data in the record can be locked, from whom, and for how long. For example, does the lock feature apply to the entire record, portions of the record or individual data elements in the record? Can a patient lock data away from specific healthcare providers? The mere presence of information hidden in a lock box may need to be disclosed so that healthcare providers understand that they do not have a patient's full medical history.

These questions will become even more challenging when EHR personal health information begins to cross jurisdictional boundaries in greater volumes. For example, if data originates in a jurisdiction where the legislation includes a lock box feature and the data is then disclosed to a jurisdiction where such a feature does not exist, is there an expectation that the receiving jurisdiction will honour the lock box provisions?

The answers to these questions have significant system development and health service delivery implications. The development of appropriate best practices in relation to lock boxes and the associated information technology standards that will be required to support the practices consistently across jurisdictions will need to be carefully considered by those responsible for EHR Infostructure governance.

---

17 Sometimes the term "masking" is used rather than "locking". In their paper, *Data Stewardship Framework, version 1.0,* September 2006, the Medical Informatics Committee of the College of Physicians and Surgeons of Alberta defines "masking" as "the application of rules that restricts access to data in an electronic record (unless additional action is taken to override the restriction)." The Government of Alberta, in their *Frequently Asked Questions: Alberta's Electronic Health Record (http://www.health.gov.ab.ca/resources/publications/QAs.pdf#search=%22EHR%20masking%22)* similarly refers to a masking function that "protects some sensitive information (i.e. the Provincial Health Officer mandated that certain laboratory test results are of a sensitive nature and should always be masked). These masked results can be viewed with a patient or agent's consent or in true emergency situations."

Defined in this way, masking is synonymous with the term "locking" as used in this paper. These terms denote a reversible process: data that has been locked or masked can, under special circumstances, be unlocked or unmasked. Regrettably, the term "masking" has also been used occasionally as a synonym for anonymisation (a process which is sometimes engineered to be irreversible) or as an informal way of referring to the process of encryption. To avoid ambiguity, this paper uses the term "locking".

18 The provinces of Ontario, Manitoba and Saskatchewan all contain masking or locking provisions in their respective health information privacy legislation.

7 Limiting Collection of Personal Health Information

Health information custodians and trustees[19] currently have a duty to limit collection of personal health information to that which is needed for identified purposes, such as treatment and care or healthcare administration. The design of the interoperable EHR must likewise limit collection of personal information. Collection of personal health information will obviously be limited by the format of the data structures implemented by the EHR Infostructure and by the format of Health Level 7 (HL7) messages used to transmit and disclose this information. Considerable work has been done by *Infoway* in developing and standardizing HL7 messages[20] but more work is needed to identify which data elements and free text reports will be retained in the EHR, which can be transmitted from a locally stored medical record (in a hospital system, for example) to the EHR Infostructure and which can be pulled from the EHR for inclusion in a hospital system or physician office system.

Issues to consider include the potential use of data fields describing family histories of disease (and hence representing information on an individual other than the record's data subject), the potential use of free-form text fields (which do not restrict the content or scope of data input), the ability to infer confidential information from the presence or absence of certain data values in ostensibly unrelated data fields (i.e., inferring a diagnosis from the name of a well-known specialist or location of a specialty clinic), and the length of time that specific health information remains clinically and legally relevant.

Future expansion of the EHR Infostructure will require ongoing governance oversight to ensure that data structures continue to respect strict limits on the collection of personal health information to what is needed for identified purposes such as treatment and care.

8 Limiting Disclosure of Personal Health Information and Privacy-Protective Grouping of EHR Data Elements

Health information custodians and trustees have a duty to disclose personal health information in a controlled manner. They may be frustrated in performing this duty if the interoperable EHR does not support a fine-grained capacity to disclose only such information as is needed in the current circumstances. On the other hand, as an individual's EHR may consist of hundreds of individual data fields, it may be impractical to disclose data by selecting data fields on a field-by-field basis. Such a selection would be very time consuming for a healthcare provider to carry out every time a disclosure were made. Moreover, some fields are related to one another and proper clinical practice would necessitate ensuring that all relevant fields were disclosed as a coherent whole. A clinically relevant and, at the same time, privacy-protective grouping of fields for the purposes of disclosure could greatly facilitate the limitation of personal health information disclosures. The satisfactory construction of such groupings that would permit the disclosure of

---

[19] For the purpose of this paper, the phrase "health information custodians and trustees" includes a “custodian” under Alberta’s *Health Information Act*, a “health information custodian under Ontario’s *Personal Health Information Protection Act, 2004*, a “trustee” under Manitoba’s *Personal Health Information Act* and Saskatchewan’s *Health Information Protection Act*, a “public body” under public sector legislation across Canada including Quebec, an organization under the *Personal Information Protection Act* in Alberta and British Columbia, and a private enterprise under Quebec private sector legislation.

[20] An example of such work is *Infoway's* CeRx project that has developed a sophisticated set of HL7 messages for the implementation of medication profiles.

more and more detailed information based on authority levels will require an effective blend of clinical and information governance.

It is also envisioned that the EHR environment may result in a shift away from the current “controlled disclosure” model contained in many statutes today to one of controlled “access.” In the current paper and non-interoperable electronic medical record (EMR) world, a primary care physician can closely control the information disclosed from a patient record. In the interoperable context, key clinical information will be accessible to authorized care providers without any intervention or control from primary care physicians. This shift will have a profound impact on the custodial responsibilities of the administrators of the EHR Infostructure, requiring them to ensure that individuals are properly authorized before they can access information at a given level of detail.

It also raises interesting questions within the context of existing legal privacy requirements. For example, section 58(2) of Alberta’s *Health Information Act* requires custodians and trustees in Alberta to consider, when deciding how much health information to *disclose*, any expressed wishes of the patient relating to disclosure of the information, together with any other factors the custodian considers relevant. Such considerations will require special attention by those responsible for access and disclosure of information through an interoperable EHR. Similar issues exist concerning healthcare providers notifying one another when information that may be clinically relevant has been locked. The determination of the clinical relevance of the information is more of a straightforward exercise in the traditional data disclosure model. However, in an automated access-based environment, where a user is interacting with a *system* rather than with another healthcare provider, the individual with access will be able to view whatever clinical data is appropriate to his or her security profile and will not benefit from “live” interaction with a disclosing healthcare provider. The management of such issues and legal requirements will require the development of appropriate policies, procedures and technologies.

9 Secondary Uses[21]

In order to allow patients to make appropriate decisions about their personal health information, it is important that they are made aware of, and understand, the purposes for which it is being collected, used, and disclosed. Consistent with the "identifying purposes principle" found in the CSA Model Code for the Protection of Personal Information and in Canadian privacy legislation, organizations connected to the EHR Infostructure and organizations hosting components of the EHR Infostructure are to identify the purposes for which personal health information will be collected, used and disclosed in a readily understandable manner, at or before the time it is collected. Such notices should not only contain a description of the purposes for which health information is initially collected (i.e., health care and treatment), but also include a description of all anticipated secondary uses of the information. The latter requirement raises three issues.

The first is that, while nearly all the information in the EHR will initially be collected for the purposes of treatment and care or for administration of the healthcare system, it is reasonable to expect that, over time, there will be interest in accessing this information for secondary

[21] The term "secondary use" generally refers to the use and disclosure of personal information for purposes other than that for which it was originally collected. Existing Canadian privacy laws generally impose a legal obligation on health information custodians and trustees to identify the purpose for which they collect, use, disclose, or retain personal health information. This may include purposes other than treatment and care; hence, so-called "secondary" purposes, i.e., medical research. Information notices given to patients, are intended to give individuals a sense of what uses are permissible.

purposes, such as public health surveillance, health system analysis and management, and research. Should patients be informed of all such secondary uses, even in situations or jurisdictions where healthcare providers are not currently required legally to do so or where the data is de-identified or anonymized? Is it reasonable to expect individuals to be apprised of potential uses in a general way, given that it is neither possible to anticipate all uses, nor to provide detail about uses that will in most cases be merely hypothetical? What level of de-identification or anonymization, if any, is needed before personal health information that was collected for the purpose of treatment and care can fairly and ethically be used for research without requiring patient consent?[22] Answering such questions for the interoperable EHR will become a governance issue as information holdings and their potential value to researchers and epidemiologists increase.

The second issue is that there are no agreed-upon best practices for informing patients in a readily understandable manner about the secondary uses of their personal health information. Current practices vary among jurisdictions and healthcare institutions. [23] As noted in relation to a number of previous topics, this matter is not unique to the EHR context. It exists already in the paper world. However, the volume of data in an EHR may lead to increased pressure by analysts and researchers to access the information. Rules regarding secondary uses of information are already set out in many laws, however, it would be valuable to review the provisions for their applicability in an interoperable EHR environment.

Finally, there are no explicit plans to include in the interoperable EHR information that would specifically indicate whether a patient agrees to be contacted for the purposes of health research. Such a field could be combined with EHR Infostructure search capabilities that searched for records of patients who had specific medical conditions and who also consented to be contacted for the purposes of health research. As the numbers of patient records in the interoperable EHR could eventually reach into the millions, the utility of such features could be valuable, especially in connection with rare conditions. Whether such potential features merit implementation will require careful consideration of the balance between protection of patient privacy, their scientific value (they could result in populations that contain bias) and the advancement of health research.

10 Patient Access to Data

The right of a patient to access his or her personal health information was affirmed by the Supreme Court of Canada in the case of McInerney v. MacDonald[24] and articulated in various Canadian privacy laws. These statutes provide patients with the general right of access to, and correction of, their records of personal health information, subject to certain exceptions.

[22] This is both a legal and a technical question. A requirement for de-identification is specified in the privacy legislation of some jurisdictions but not others. No jurisdiction specified the technical details of, for example, pseudonymisation. An ISO standard forthcoming in 2007 addresses the application of this technology to health care in detail.

[23] At a minimum, health sector specific privacy laws require that healthcare organizations identify a contact person, often known as a Privacy Officer, to ensure overall privacy compliance. In addition, policies and procedures must be established in order to promote knowledge and awareness of the privacy rights of individuals, which could include secondary uses of their personal health information. The actual content of such policies, however, vary among jurisdictions. Generally accepted practices may vary even among healthcare institutions within a given jurisdiction, based on the different patient client populations served by various healthcare providers and organizations.

[24] *McInerney v. MacDonald,* [1992] 2 S.C.R. 138.

Access by Patients to the Full Content of Their EHR

Patients wanting access to all their personal health information could obtain it from all its original sources: i.e., medical history from a family physician, medication profile from a provincial repository such as the Alberta Pharmacy Information Network or BC Pharmanet, hospital records from every hospital visited, diagnostic images from a regional repository, lab tests from a provincial repository such as the Ontario Laboratory Information System, etc. But once the interoperable EHR is in place, information will be available through the shared record. Jurisdictions will need to consider access and correction policies related to the EHR at the local as well as at the "pan-Canadian" level.

Online Access by Patients to Portions of Their EHR

There is already considerable discussion about the potential of the EHR to provide patients direct online access to their own clinical information. There may be some portions of the record that are amenable to direct, unmediated access—demographic data is an obvious example, and the management of chronic diseases, such as diabetes and HIV/AIDS, provide a potential opportunity for patients to review online the results of routine, recurrent tests. However, in other cases, there may be a need for a primary care provider to interpret the record's content, provide counselling and help the patient understand the healthcare implications of the data. The question as to what personal health information, if any, is amenable to unmediated online access by patients remains outstanding, but will need resolution as interoperable EHR initiatives continue to develop.

Patients Challenging Accuracy

Most jurisdictions allow patients to challenge the accuracy or completeness of their personal health information. If patients are provided with access to their EHR, even in a limited or mediated fashion, the EHR Infostructure may need to include a mechanism to facilitate compliance with this legal requirement and to help organizations respond to such requests within the legally required time. Clear procedures will also be needed to regulate access by substitute decision makers.

2.4 Topics Related to Assessment and Compliance

11 Determining Acceptable Levels of Risk

Threat and Risk Assessments (TRA) and a Privacy Impact Assessments (PIA) are processes by which specific privacy and security issues and mitigating strategies can be identified. They have become common tools for assessing compliance with information governance obligations.

Generally, PIAs identify the privacy requirements and data flows relating to the information system in question; they identify risks that the information system and associated people and processes pose to individual privacy; and; they also propose mitigating strategies to reduce or eliminate these risks. Since privacy risks in large information systems can rarely ever be completely eliminated, such assessments are not intended to be static documents, but ones that need to be continuously reviewed and updated. The implementation of the risk mitigation strategies needs to be tracked and new risks identified and corresponding mitigation strategies developed as they arise. Although substantial expertise exists across Canada in the conduct of PIAs, few best practices or policies have been developed to monitor the implementation of privacy risk mitigation strategies and to integrate privacy monitoring and PIA revisions into the change management process. Developing programs to ensure continuous privacy management is an issue that will need to be addressed as part of effective EHR information governance.

Security-related risks can never be completely eliminated in any complex IT system. Every risk identified in a TRA needs either to be mitigated (i.e., by adding additional security controls), transferred (i.e., by outsourcing a service component to an agency or third party better equipped to deal with the risk), or accepted (i.e., by informing users that files stored on a given server will only be backed up once per day). A TRA often begs the question, what level of residual risk is acceptable? In relation to the EHR Infostructure, questions about the acceptability of residual risks have remained largely unanswered. For example, while most observers agree that users of EHR Infostructure services must be authenticated, there is no broad agreement on the level of authentication for access to these services.

Effective information governance will require considering how often PIAs and TRAs should be conducted, as well as their breadth and depth, for the EHR and portions thereof as well as answering questions about acceptable risk levels.

12 Compliance Mechanisms

Acceptable use agreements and confidentiality agreements for users of EHR systems are important tools for requiring compliance with privacy and security policies. As personal health information flows across jurisdictions via the EHR Infostructure, any major discrepancies from one jurisdiction to another may impair the ability of EHR Infostructure administrators to hold users accountable for their actions. Many Canadian healthcare organizations are already using such agreements for access to data holdings. It would be valuable to study some of the documents currently in use and develop a template or inventory of features to be included in such agreements.

13 Liability and Sanctions

An important aspect of ensuring compliance is the presence of sanctions. For example, Manitoba makes it an offence for any trustee to collect, use, sell or disclose personal health information contrary to the province's *Personal Health Information Act*. Saskatchewan's health privacy legislation provides substantial penalties for wilful breaches of up to $500,000 for corporations. Unlike other provinces, Saskatchewan also expressly provides for imprisonment for up to one year in addition to any financial penalty levied upon individuals. Ontario also has tough penalties for breaches of its health information privacy act: upon conviction, a person guilty of an offence is subject to a fine of up to $50,000 and corporations may faces fines of up to $250,000. Most statutes also provide protection from liability where health information custodians and trustees acted in good faith or took reasonable steps under the circumstances to prevent a privacy breach from occurring.

In addition to the issue of how sanctions from multiple jurisdictions would apply if an offence involved transborder data flows, there is the larger issue of a sanction's effect on ensuring compliance with information governance policies. In jurisdictions that lack sanctions established in privacy statutes, there is also the question of whether common-law settlements for "actual harm" are substantial enough to act as an effective deterrent. In light of the large volumes of personal health information that a user of the interoperable EHR could potentially access, should there be specific penalties for the misuse of personal health information in the interoperable EHR context? Should patient identity theft be deterred by laws or regulations that explicitly protect patient directories from such exploitation? The development of broad consensus on such issues could inform future amendments to privacy acts or criminal law.

Healthcare providers have always been bound by ethical and legal duties to maintain the confidentiality of health information, even prior to the enactment of privacy legislation. Professional misconduct regulations and codes of ethics[25] of regulated healthcare providers have specific provisions dealing with confidentiality of patient information, breach of which can lead to disciplinary and other professional conduct sanctions. Regulatory bodies are legally required to set professional standards for healthcare practitioners, which include practice standards for confidentiality. Depending on the severity of the breach, a breach of an ethical duty or a standard of conduct may be relevant to an action in negligence. [26] Professional standards of practice do not yet explicitly address use (or misuse) of EHR systems and related technology although some regulatory bodies have begun to examine issues relating to the appropriate use of information technology.

14 Assessment of Information Governance

How will compliance with information governance policies and practices be assessed? In the UK health trusts and hospitals extensive use is made of self-assessment tools for measuring the effectiveness of information governance.[27] Such assessments are used in the UK National Health Service as a basis for planning, making incremental improvements and achieving the goal of uniformly high quality information governance. Such assessments are not done in Canada. Nor is data readily available, as in the UK, on how well healthcare institutions and primary care practices adhere to their own privacy and security policies.

Some jurisdictional privacy laws assign health information custodians and trustees specific obligations that are absent in other jurisdictions. For example, Manitoba-based trustees must conduct privacy training for staff, but equivalent officials in most other provincial jurisdictions have no legal obligation to do this. The scope of compliance assessment may, therefore, vary from one jurisdiction to another. Nevertheless, to the extent that a common core of requirements can be assembled and maintained, much duplication of effort could be eliminated by formulating appropriate approaches to assessing compliance.

2.5 Topics Related to Quality in Health Care

15 Accuracy and Data Quality

Everyone occasionally make mistakes. But when mistakes are made in diagnoses, test results, or medical histories, not only must they be corrected, but the corrected errors also need to be reported to other healthcare providers who may have taken action based on the erroneous data. The EHR Infostructure has been designed to "push" updated information to users upon their request. In systems being implemented with this feature, users who subscribe to the service

---

25 See for example, Canadian Psychiatric Association, *The Confidentiality of Psychiatric Records and the Patient's Right to Privacy*, at: http://www.cpa.apc.org, and Canadian Nurses Association, *Code of Ethics for Registered Nurses* at http://www.cna-nurses.ca/CNA/practice/ethics/code/default_e.aspx.

26 See for example, the case of *Peters-Brown v. Regina District Health Board* [1995] S.J. No. 60 (Sask. Q.B.) where a hospital was found negligent in posting confidential information and *Hay v. University of Alberta Hospital* [1990] 5 W.W.R. which confirmed the existence of a tort action for breach of confidentiality: "A physician who divulges confidential information could face an action for breach of confidentiality…."

27 See www.igt.connectingforhealth.nhs.uk

would be alerted of an update to the information. The system would not automatically notify all who accessed the original information before it was updated. An automatic update may be the best way of ensuring that corrections to erroneous data will come to the attention of users who have previously accessed the data in its erroneous form. In any event, healthcare providers need to know what mechanisms will be put in place to automatically promulgate important updates such as changes to lab test results and to notify those who have previously accessed the erroneous information. The procedural details of how this is accomplished (for example, what constitutes an "important" update) in the various phases of EHR Infostructure deployment must be carefully worked out.

The EHR Infostructure architecture is based on the (unstated) assumption that all the sources of its data are definitive and of equal quality. In reality, this is unlikely to be true. Jurisdictions that systematically assess institutional quality of care and make their findings public have shown that data quality and effectiveness of health records management vary from hospital to hospital, just as other quality indicators do. Could there be minimum criteria for data quality that, if not met, would result in a healthcare institution being cut off as a data source for the interoperable EHR? Might a future version of the EHR Infostructure include a quality indicator for its data sources? Might clinicians one day be able to record a subjective confidence factor along with a diagnosis? Such questions are contentious because they challenge broadly held assumptions about the objectivity and uniform high quality of medical data. Nevertheless, as the interoperable EHR evolves to encompass a wide range of data sources and elements, these questions may need to be addressed. Good answers will only come from an effective integration of clinical and information governance.

16 Data Retention, Archiving and Disposal

Statutes that dictate the length of time health records must be kept by a variety of health information custodians are in place. Good privacy practices require that personal information should be retained only as long as necessary. Sound health records management practices dictate that health records be archived when not actively in use and that archives be retained for as long as their content could reasonably be expected to be accessed. Within this mix of legal requirements and best practices, discussion will be necessary to determine the appropriate length of time to keep data in the interoperable EHR context. EHR data could be expected to be accessed throughout a patient's life, and potentially well after the patient’s death. Should the data remain accessible online in an interoperable EHR? Or should it instead be electronically archived with special access being granted to the archive upon request?

The rapidly falling price of online storage has frequently forestalled the need to make hard decisions about archiving, as the cost per byte continues to fall by 50 per cet per year. Also, most electronic repositories of personal health information are not very old. But the need for clear guidelines on both retention and archiving will eventually catch up to repositories of electronic health information. Guidelines will also be needed on the technical safeguards needed to secure archives and on ways to ensure digital signatures that have been applied to archived material remain tamperproof for the lifespan of the archive (see topic 19 for a discussion of digital signatures).

2.6 Topics Related to Technical Safeguards

17 Access Controls

Access controls[28] include identification of users during registration, their subsequent authentication during log-in and their authorization prior to being granted access to services and data. Access controls can also be structured to reflect the context in which the individual is working. For example, a nurse working in a hospital may have one set of authorizations while the same nurse working in a long-term care facility would have a different set of authorizations. Access control is intended to prevent unauthorized access to information systems, ensure the protection of services, prevent unauthorized computer access, detect unauthorized activities and ensure information security when using mobile computing and tele-networking facilities. The interoperable EHR creates unique challenges for access control as the number and variety of its users will be considerably larger than for a medical record system in a physician office or hospital. One particularly challenging aspect of expanding existing systems of access control from physician office and hospital-based systems to the interoperable EHR will be to effectively establish user roles for EHR Infostructure users.[29] Although healthcare providers are usually regulated healthcare professionals whose credentials can be obtained from regulatory colleges, other potential users, such as medical receptionists, draw their authority to retrieve or update portions of the EHR (demographic information, for example) from another healthcare provider (for example, a physician in a solo practice who has employed the receptionist). Anchoring this "chain of authority" to a regulated healthcare professional or officially recognized custodian or trustee is an important component of ensuring accountability for personal health information. Such maintenance, in turn, may involve primary care providers and others in the EHR Infostructure user registration process and hence may add considerable complexity to the process, extending far beyond the simple model of relying on provider registries drawn from the licensed credentials of the jurisdictional regulatory colleges.

Technically, three mappings would greatly facilitate the implementation of role-based access control in the EHR Infostructure:

1. A mapping of user roles for a local information system (i.e., a hospital EHR system) to user roles for the EHR Infostructure: For example, in order to access personal health information in a medical emergency, some users of the EHR Infostructure will need emergency override privileges. The EHR Infostructure users who will be given these override privileges are the ones with a role, for example, of "Emergency medicine." In a given hospital's patient record system, the user roles to be granted such override privileges will presumably be the roles given to users in the emergency department. But

---

[28] See Canada Health Infoway, *Electronic Health Record Infostructure Privacy and Security Conceptual Architecture, Version 1.1, June 2005*, p. 16 for more discussion of access controls for the EHRi.

[29] Among the types of access control discussed in *Infoway's* Privacy and Security Conceptual Architecture, role-based access control is especially important as a component of the overall EHRi access control strategy. This form of access control assigns each user to one or more user roles. Each user role is then mapped to one or more EHRi access privileges. The access privileges consist of sets of data fields and associated access modes (read-only, update, etc.), and sets of EHRi capabilities (patient search, etc.). By judiciously defining a limited number of roles and mapping them to a manageable set of access privileges, administrators can quickly assign each user precisely those access privileges needed by someone in that user's role. The alternative – assigning privileges to users on an ad hoc, user-by-user basis – has historically been shown to be unwieldy, error-prone, and insecure.

which roles are they? In one hospital, they may be roles such as "Emergency Department physician," or "Emergency admitting clerk." In another hospital, it may be the role "Emergency department user." In yet another hospital, it may be "Role number 6." At the moment, there is no consistency in the titles or definitions of user roles from one institution to another, even within the same jurisdiction. Thus, a mapping from organizational user roles to EHR Infostructure user roles will be important and requires a common standard.

2. A mapping of user roles in the EHR Infostructure to the specific access privileges associated with the role: For example, if there is an EHR Infostructure user role called "Registration clerk/Admitting clerk," a user assigned this role will presumably be able to access demographic information and perform patient searches by name, etc. Will these users also be able to access a patient's medical history? A privacy advocate might argue that clerks have no need to see detailed medical information. A hospital administrator might argue that an admitting department clerk will want to make sure that a patient presenting with certain symptoms (i.e. SARS-like symptoms) or a patient who has been prescribed certain medications (i.e. antibiotics associated with certain contagious diseases), is admitted to an infectious diseases screening area. Such discussions of role-based access control often require a careful balance between privacy and security on the one hand, and clinical and administrative utility on the other.
3. A partial mapping of roles and access privileges from one jurisdiction's implementation of the interoperable EHR to another's for all jurisdictions permitting access from users in another jurisdiction: It cannot be assumed that all jurisdictions will settle on the same list of roles and access privileges. Therefore, a cross-jurisdictional mapping is needed for at least some user roles and privileges.

Working out these mappings is a complex exercise but role-based access control is fundamental to the effective functioning of the interoperable EHR.

18 Auditing, Security Incident Handling and Privacy Breaches

Given sufficient time, security incidents and privacy breaches will inevitably occur in any large and complex IT system. Security incidents include contamination by viruses and malware, intrusion detection and system failures or denial of service attacks that lead to EHR services becoming temporarily unavailable to users. Security incidents can also occur when ostensibly authorized users behave in a suspect fashion, i.e., repeatedly accessing records for patients with whom they have no established relationship. These incidents may only come to light when audit logs are carefully reviewed. Some security incidents result in privacy breaches. Four issues related to auditing, security incident handling and privacy breaches need discussion and resolution; they are outlined below.

Timely Handling of Security Incidents in the Interoperable EHR

Time is usually of the essence in responding effectively to both security incidents and privacy breaches, so continuously monitoring systems for intrusion detection is an important component of robust security. Personnel and procedures should be in place to respond immediately to any apprehended security incident or privacy breach. Responsibilities for the handling of security incidents and privacy breaches will need to be carefully delineated, especially in interconnected systems that cross organizational and jurisdictional boundaries.

Real-Time Auditing

Although audit logging is an essential feature of secure systems, the logging of active attempts at system intrusion raises the more general issue of who will review logs, especially real-time logs that require round-the-clock system support. The apportioning of system support tasks between local and jurisdiction-wide systems and inter-jurisdictional systems, such as the Health Information Access Layer[30], is not addressed in the EHRS Blueprint. Responsibilities must be carefully delineated so that the entire EHR Infostructure remains continuously defended against intrusion. Even routine (i.e., non-real-time critical) logging of events merits routine, scheduled review and analysis. This process also raises issues about responsibilities for the audit of inter-jurisdictional information flows on a regular and timely basis.

Real-time or near-real time auditing may also be used to protect patient privacy. For example, some EHR Infostructure applications are designed to require users to provide a reason as to why they require access to personal health information that has been locked. This information is immediately transmitted to an identified individual, such as the organization's privacy officer. In addition, the technology now exists to create a similar alert when a healthcare provider accesses information on a patient with whom they have no prior clinical relationship and no readily apparent need-to-know (i.e., his or her active role does not involve emergency medicine and he or she is not within the patient's established "circle-of-care"). The level of sophistication and sensitivity of alerts and the resources needed to review and respond to them are all information governance issues that will need to be addressed.

Preservation of Digital Evidence

On rare occasions, the contents of health records are entered into evidence in judicial proceedings or inquests. Electronic health records have evidentiary requirements that they must meet in such situations. While these requirements are often the same as for paper records, there are additional procedures required to maintain a chain of evidence for data stored solely in electronic form. The *Infoway* Privacy and Security Conceptual Architecture already contains basic provisions for ensuring the integrity of records, controlling access and ensuring that a complete time-stamped audit of changes to each record will ensure that historic record content can be reconstructed as it existed at any point in time. But fully elaborated procedures and guidelines have not been developed for maintaining a demonstrably intact chain of evidence when complying with court orders. There may be other evidentiary requirements that the EHR Infostructure must meet in the future.

Privacy Breaches

Some security incidents lead to privacy breaches. Systems should be able to help determine the nature and extent of any such breach. Guidelines should also be implemented to help staff know when and how patients are to be notified of a privacy breach. Premature notification of a purported breach may lead to loss of confidence in the interoperable EHR, especially if the breach is a false alarm. Conversely, undue delays may also lead to loss of confidence and may increase the risk of successful identity theft if the personal information obtained includes data needed for identity theft (name, address, date of birth, mother's maiden name, phone numbers, etc.). The notification process then needs to be conducted in a privacy-protective manner.

[30] The Health Information Access Layer (HIAL) is a collection of technical services that allow personal health information to be accessed by an EHRi user. It also acts as a filter to ensure that personal health information is never disclosed inappropriately. For example, access control is part of the HIAL.

Ontario is the only Canadian jurisdiction to date that requires custodians to notify affected patients at the first reasonable opportunity if their personal health information is stolen, lost or accessed by unauthorized persons.[31] The Ontario Information and Privacy Commissioner has published a paper on what to do when a privacy breach occurs which focuses on containment and notification as two avenues of appropriate action.[32]

19 Electronic (Digital) Signatures

Federal law and regulations currently require a prescriber's signature on written prescriptions. *Infoway* and Health Canada have jointly investigated the possibilities for allowing digital signatures on electronic prescriptions.[33] If laws and regulations were changed to permit this use, digital signatures could allow the introduction of electronic replacements for paper-based documents such as prescriptions, lab requisitions, clinical notes and death certificates, that is, documents normally requiring a healthcare provider's signature.

Digital signatures require the one-time issuance[34] of digital certificates to the signatories by a qualified entity typically referred to as a *certification authority*. The certification authority issues the certificates by adhering to a specific certificate policy. Such certificate policies typically have a standard format. Indeed, there is a Canadian standard on the issuance of digital certificates.[35]

If digital signatures are allowed on prescriptions, who should serve as certification authorities for healthcare providers and what should the specifics be of the certificate policy or policies? The joint report by Health Canada and *Infoway* recommends that such certificates "be issued by a certification authority approved by a provincial or territorial regulatory college to issue digital signature certificates to members of that college for purposes including the signing of prescriptions in electronic format."[33] No such certification authorities have yet been approved in this manner though both the Saskatchewan Health Information Network and Smart Systems for Health Agency have already issued digital certificates to their users (extensively in the former case and in a limited fashion in the latter).

---

[31] Section 12(2) and 17(3) of Ontario's PHIPA, respectively.

[32] See Information and Privacy Commissioner/Ontario, *What to do if a privacy breach occurs: Guidelines for government organizations,* May 2003; available at: http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=14323&U_ID=0

[33] The issues are fully explored in Canada Health Infoway, Health Canada, *Ensuring the Authenticity of Electronic Perscriptions: Proposed Approach*, 2006.

[34] Once issued, a digital certificate can be used by a signatory to sign an unlimited number of electronic documents. Digital certificates typically have expiry dates however to ensure that technical advances do not render the associated cryptographic keys insecure. The certificates must, therefore, be renewed by the certification authority before expiry.

[35] The standard consists of three parts:

I. CAN/CSA-ISO/TS 107090-1 *Health Informatics - Public Key Infrastructure. - Part 1: Framework and Overview* (Adopted ISO/TS 17090-1:2002, first edition, 2002-10-15)

II. CAN/CSA-ISO/TS 107090-2 *Health Informatics - Public Key Infrastructure. - Part 2: Certificate Profile* (Adopted ISO/TS 17090-2:2002, first edition, 2002-10-15), and

III. CAN/CSA-ISO/TS 107090-3 *Health Informatics - Public Key Infrastructure - Part 3: Policy Management of Certification Authority* (Adopted ISO/TS 17090-3:2002, first edition, 2002-10-15)

The joint paper also explores alternatives to digital signatures. Before pursuing an alternative, its risks need to be carefully assessed, lest an alternative be chosen that poses unacceptable risks of prescription fraud.

2.7 Topics Related to the Rights of Healthcare Providers and Communities of Interest

20 User Identity Management and Protection of Healthcare Provider Privacy

It is a truism of access control that if access to an IT system is to be limited to authorized users, then one must know in advance who all the authorized users are. This requires the registration of users and their enrolment in one or more programmes or IT services. To confirm the identities of potential users prior to registering them, large amounts of personal identifying information are often collected. This information may include name, address, contact information such as phone numbers, license numbers associated with professional practice, and other personal identifiers. If it is not properly protected, this data can potentially be stolen and then used to commit identity theft. Collecting such data, therefore, carries with it the burden of ensuring that it is effectively safeguarded. Users should be informed of the purposes for which this data will be collected and used, and; use of the data then limited to those purposes. In short, the principles of the CSA Model Code also apply to registration and enrolment data.

In addition to concerns about identity theft, healthcare providers and institutions may also have concerns about the monitoring of their patterns of practice Healthcare providers generally welcome statistical studies of practice patterns, provided these studies have been approved by research ethics boards[36]. Such approved studies protect healthcare provider anonymity. Uptake of the interoperable EHR may be hampered if healthcare providers fear that the data collected will be used to evaluate their competency or judge their standards of practice unfairly. Assuaging such fears will, therefore, be an important component of trustworthy information governance.

21 Respecting Communities of Interest

Much discussion of privacy rights in health care today is focussed on the rights of individual patients. Such discussion often overlooks the role played by specific communities. It wasn't always so. The history of patient privacy rights in Canada began within the mental health community. Advocates for the rights of mental health consumers were joined in the late 1980s by advocates of the rights of people with HIV/AIDS. Both groups attached paramount importance to patient-centred control of healthcare information and the right to privacy. Individuals who needed treatment or counselling also needed to have sufficient trust in the healthcare system to allow them to seek treatment without fearing loss of their privacy.

[36] Research ethics boards (REBs) currently serve the function of gatekeepers in approving health research studies and ensuring that the confidentiality of research data is protected. In Manitoba, for example, a Health Committee created under provincial law must authorize all data requests for research purposes. In Ontario, research is permitted without patient consent so long as the privacy requirements respecting research under PHIPA and its corresponding regulation are met. This involves the health information custodian or trustee preparing a research plan for approval by an REB, which includes a description of the research proposed to be undertaken and the duration; why consent to the disclosure of personal health information is not being sought; a listing of all persons who will have access to the information, why their access is necessary, and their roles in relation to the research and their related qualifications (see section 16 of the Regulation made under PHIPA: O. Reg. 329/04, amended to 245/06).,

Community organizations successfully sought to ensure patient rights by integrating community involvement into the governance of the relevant healthcare organizations. This involvement is now customary for the governance of institutions involved in mental health and addictions. For example, the board of the Canadian Mental Health Association has had a consumer advisory council since 1987.

This trend to community participation can also be seen in the governance of AIDS organizations. For example, the Ontario HIV Treatment Network (OHTN), a provincially funded not-for-profit organization, is chartered in a way that ensures that more than 50 per cent of its board of directors' voting members are community representatives. Especially at the time the OHTN was formed, such community participation was necessary to ensure the trust and participation of consumer-based organizations.

Mental health consumers and people with HIV/AIDS are not the only ones to demand a role in the governance of healthcare organizations. The struggle to improve the health and welfare of Aboriginal Peoples has also led to the involvement of aboriginal communities in the governance of health information initiatives such as the Aboriginal Health Reporting Framework. First Nations Peoples will continue to have a crucial voice in the collection, use and disclosure of personal health information within their communities. Effective information governance of such initiatives will involve more than the typical discussion of individual patients' rights that goes on in non-Native communities. It will also involve discussion of the rights of Native communities as a whole in the ownership, access, control and possession of personal health information[37].

Finally, lessons learned from the struggles to advance the rights of the mentally ill have shaped provincial and territorial mental health acts. Many of these mental health laws predate Canadian privacy laws and they are sometimes more demanding in their precepts than are analogous privacy laws or have been amended to make the provisions of a subsequent privacy law even more protective of patient rights. For example, regulations under the Ontario Mental Health Act[38] specify rights for patients who have been deemed incapable of consenting to the collection, use and disclosure of personal health information under Ontario's Personal Health Information Protection Act, 2004. No serious attempt can be made to include mental health data in the interoperable EHR without attending to the impact mental health laws and regulations will have on information governance.

[37] Some privacy advocates refer to "group privacy rights" in contradistinction to individual privacy rights.

[38] R.R.O. 1990, Reg. 741

3. REQUIREMENTS FOR INFORMATION GOVERNANCE IN CANADIAN HEALTH CARE

3.1 Introduction

The previous chapter identified 21 information governance topics with implications for the privacy and security of personal health information in the interoperable EHR. This chapter describes some of the legislation, ethical principles and policies that currently influence information governance in the Canadian health care system.

Health information governance is informed by a combination of legal, ethical and regulatory requirements for the collection, use or disclosure of personal health information, among others. The current privacy framework that applies to healthcare providers is made up of the following:

- Privacy laws and regulations in effect in different Canadian jurisdictions;
- Health-related legislation with specific confidentiality provisions or with restrictions on the collection, use or disclosure of personal health information (i.e. provincial public hospitals acts or medical care insurance acts that either prohibit third-party disclosures or contain specific confidentiality provisions);
- The Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96);
- Professional codes of ethics and health privacy codes or guidelines created by health professional associations and professional standards of practice and professional misconduct regulations set by the health regulatory colleges; and
- Common law medical confidentiality obligations and administrative rulings issued by professional regulatory colleges and by Information and Privacy Commissioners.

Section 3.2 describes some of some of the legislative and ethical requirements for privacy and security of personal health information. Section 3.3 analyses the implications of these rules and requirements on information governance. As the reader proceeds through these next two sections, two challenges should become apparent. The first is that while existing legislation covers many privacy and security issues, the approaches taken are not always consistent with one another. This may lead to challenges in managing EHR data as it moves from one jurisdiction to another unless legally acceptable principles can be agreed to. The second is that the rules and their variations can be perplexing to front-line healthcare providers. Agreement on overarching principles would help everyone — health care providers, oversight bodies and the public — understand the rules under which the interoperable EHR is governed.

3.2 Legal, Ethical and Professional Standards for Protecting Privacy

Insofar as there are existing information governance requirements that are mandated by law, designers of a pan-Canadian interoperable EHR will build on these when contemplating various information governance solutions. None of the requirements and best practices described in this section deals with *all* of the information governance topics identified in Chapter 2, at least not in the level of detail required to truly support a pan-Canadian interoperable EHR. Instead, they provide a starting point for the development of future information governance solutions.

Privacy and the Charter of Rights

While the Charter does not explicitly provide a right to privacy, the Supreme Court of Canada recognizes that a right of privacy exists in Canadian law. For example, section 8 of the Charter, which provides individuals with the right to be secure against unreasonable search or seizure by the government, and section 7, which guarantees individuals the right to life, liberty and security of the person, provide a source of constitutional protection for the right to privacy. For example, in R. v. O'Connor ([1995] 4 S.C.R. 411), the Court recognized that individuals have a reasonable expectation of privacy in therapeutic records, such as medical or counselling records. In her reasons, Justice L'Heureux-Dube stated that "respect for individual privacy is an essential component of what it means to be “free” and that "the infringement of this right undeniably impinges upon an individual's liberty." There are numerous Supreme Court of Canada decisions that have spoken to the right of privacy.[39] The Quebec Charter of Human Rights and Freedoms also contains a right to respect for private life in article 5 and the right to non-disclosure of confidential information in article 9.

Privacy Acts

The protection of personal health information is regulated by various privacy laws across Canada which, in turn, establish standards both for health information governance and for patient privacy rights. For example, most provinces and territories have enacted freedom of information and protection of privacy statutes to protect personal information in the custody or control of public or government bodies, including publicly funded healthcare sector entities, such as hospitals, and, in such jurisdictions where they exist, regional health authorities or health agencies. These include the Northwest Territories’, Yukon’s, Nunavut’s as well as Newfoundland and Labrador’s *Access to Information and Protection of Privacy Act*, Saskatchewan’s *Freedom of Information and Protection of Privacy Act*, Alberta’s *Freedom of Information and Protection of Privacy Act*, British Columbia’s *Freedom of Information and Protection of Privacy Act*, Nova Scotia’s *Freedom of Information and Protection of Privacy Act*, New Brunswick’s *Protection of Personal Information Act,* and Prince Edward Island’s *Freedom of Information and Protection of Privacy Act.* Quebec also has an *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* which applies to public bodies and health institutions.

Similarly, the federally regulated public sector has privacy legislation in place to cover both personal information and personal health information in the custody and control of federal government bodies (i.e. the *Privacy Act*). There also exists federal private sector legislation, namely the *Personal Information Protection and Electronic Documents Act* (PIPEDA), that applies to both federal and provincial entities in the course of conducting commercial activities, unless provincial privacy statutes have been deemed to be substantially similar (in which case the provincial statute applies).[40] (As of September 2006, the Government of Canada has deemed the privacy legislation in Quebec, the private sector privacy legislation in British Columbia and Alberta and the health information specific legislation in Ontario to be

[39] The Supreme Court of Canada has also suggested in R. v. Beare ([1988] 2 S.C.R. 387) that section 7 of the Charter includes a right to privacy not unlike that found in section 8. Another example is the case of R. v. Mills ([1999] S.C.J. No. 68), where Iacobucci and McLachlin JJ. stated that "in cases where a relationship is threatened by the disclosure of private records, security of the person and not just privacy is implicated."

[40] The Government of Canada has deemed the privacy legislation in Quebec, BC, Alberta, and Ontario to be “substantially similar” to the requirements of PIPEDA.

'substantially similar' to the requirements of PIPEDA.) As such, PIPEDA applies to information collected, used or disclosed 'in the course of commercial activities in the health sector and most specifically to information collected, used or disclosed by private pharmacies, laboratories and healthcare providers in private practices.[41]

Currently, there are four provinces, namely Alberta, Manitoba, Ontario, and Saskatchewan, that have enacted legislation specific to health information and that contain specific rules relevant to electronic health records. These laws are:

- The *Health Information Act*, Alberta (HIA);
- The *Personal Health Information Act*, Manitoba (PHIA);
- The *Personal Health Information Protection Act,* Ontario (PHIPA); and
- The *Health Information Protection Act*, Saskatchewan (HIPA).

Alberta, British Columbia and Quebec have private sector privacy legislation that protect personal information, including health information held by private health sector entities, including pharmacies, laboratories and private clinics (the *Personal Information Protection Act* and *An Act respecting the Protection of Personal Information in the Private Sector,* respectively). Quebec also protects personal health records held by public and private health and social service institutions by *An Act respecting Health Services and Social Services*. Alberta is the only province with both a general private sector law and a health specific law.

In an attempt to harmonize existing Canadian privacy regimes, the Federal/Provincial/Territorial Conference of Deputy Ministers of Health tasked its Advisory Committee on Information and Emerging Technologies (ACIET) with developing the *Pan-Canadian Health Information Privacy and Confidentiality Framework* ("the ACIET Framework").[42] The ACIET Framework provides guidelines for common and consistent statutory provisions for the collection, use and disclosure of personal health information. The framework applies to both the public and private healthcare sectors and serves as a tool for regulators as they look to develop consistent privacy requirements through the introduction or amendment of health privacy legislation. The ACIET Framework was finalized in January 2005 and endorsed by the Federal/Provincial/Territorial Conference of Deputy Ministers of Health with the exception of Saskatchewan and Quebec. The ACIET Framework continues to serve to inform and influence the development and review of health privacy statutes in Canada.

Other Relevant Acts and Statutes

Physicians and other healthcare providers are bound by other statues as well. For example, in Ontario, physicians are bound by the *Medicine Act* and nurses are bound by the *Nursing Act*. Public hospitals in Ontario are bound by the *Public Hospitals Act*, which confers several governance requirements and responsibilities on the boards of directors for the public hospitals which the Act covers. These governance responsibilities include everything from rules on financial reporting to the compilation of medical records. Within this governance framework,

---

[41] PIPEDA Awareness Raising Tools (PARTs) located at http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/en.gv00211e.html, question #9.

[42] The federal/provincial/territorial Health Ministers created ACIET in 2002 consisting of representatives from all F/T/P governments, Health Canada, Canadian Institute for Health Information, the National Aboriginal Health Organization and Canada Health Infoway. See Advisory Committee on Information and Emerging Technologies (ACIET), *Pan-Canadian Health Information Privacy and Confidentiality Framework*, Ottawa: Health and the Information Highway Division, Health Canada, January 2005. Available at http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html .

however, public hospitals in Ontario are also bound by the *Personal Health Information Protection Act, 2004* (PHIPA). Other jurisdictions have similar overlapping legal requirements.

Legislation may establish a healthcare organization or facility, but leave the details of a privacy and security regime for a future regulation. For example, the *Centre for Health Information Act* (CHIA) in Newfoundland and Labrador sets out the objects for the Centre for Health Information (the "Centre") which is responsible for assisting individuals, communities, health service providers and policy-makers at the federal/provincial/regional levels in making informed decisions to enhance the health and well-being of persons via a comprehensive province-wide health information system. The Act itself does not, however, establish the privacy framework for how the Centre is to fulfill its corporate objects in handling personal health information via its network. These privacy rules have been left to regulation. In Newfoundland and Labrador, neither the CHIA nor the privacy provisions of the *Access to Information and Protection of Privacy Act,* which apply to public healthcare bodies, have been proclaimed. As such, the Centre, as well as other healthcare providers, relies upon a key privacy document entitled *Privacy, Confidentiality and Access to Principles and Guidelines for the Health Information Network*[43] for a privacy framework with respect to health information.

Model Code for the Protection of Personal Information

While Canadian privacy laws are lengthy and complex, most are based on internationally accepted fair information principles which form the basis for the 10 privacy principles of the Canadian Standards Association's Model Code for the Protection of Personal Information (CAN/CSA-Q830-96). These principles are widely regarded as an important information governance model[44]. They are:

1. Accountability for Personal Information
2. Identifying Purposes for the Collection of Personal Information
3. Obtaining Consent
4. Limiting the Collection of Personal Information
5. Limiting the Use, Disclosure, and Retention of Personal Information
6. Ensuring the Accuracy of Personal Information
7. Ensuring Safeguards for Personal Information
8. Granting Individuals Access to their Personal Information
9. Openness and Transparency about Personal Information Practices
10. Challenging Compliance

The principles above tend to work well when applied to information held within a single organization. They may be more difficult to apply to the interoperable EHR, however. For example, it is an essential principle of the CSA Model Code that organizations that collect, use

[43] Newfoundland and Labrador Centre for Health Information, *Privacy, Confidentiality and Access to Principles and Guidelines for the Health Information Network*, October 2004; available at: http://www.nlchi.nf.ca/pdf/principles_guidelines_revised2004.pdf#search=%22Privacy%2C%20Confidentiality%20and%20Access%20to%20Principles%20and%20Guidelines.%20%22

[44] British Columbia Ministry of Labour and Citizens' Services, *PIPA Tool: Ten Principles for the Protection of Privacy*"; available at: http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/PIPA_Tool_4.htm

or disclose[45] personal information clearly identify individual(s) responsible for ensuring compliance with applicable data protection legislation and institutional privacy policies (principle 1 above). In health care, health-sector-specific privacy laws require healthcare organizations to identify a contact person (commonly known as a Privacy Officer) to ensure overall privacy compliance and to establish policies and procedures in order to promote knowledge and awareness of the privacy rights of individuals, including administrative, technical and physical safeguards to protect the integrity, accuracy and confidentiality of personal health information[46]. Healthcare providers are also responsible for ensuring that employees, staff and volunteers comply with the privacy law in each respective jurisdiction. [47,48,49,50] Manitoba, for example, requires trustees to provide orientation and ongoing staff privacy training to ensure that employees in this jurisdiction sign a pledge of confidentiality.[51]

In the interoperable EHR context, where personal health information is exchanged among multiple health care organizations within the same jurisdiction or where frequent exchanges of personal health information occur among closely related institutions, it may be reasonable to consider designating one contact person. Under PHIPA in Ontario, certain health information custodians that operate more than one facility, program or service can be listed under 3(6) of the Act to be a "single health information custodian." This means that multiple healthcare facilities can adopt a common, unified approach to privacy by, for example, designating one common contact person to facilitate compliance and developing a common standard policy for use across all sites. PHIPA also provides ways in which other health information custodians who are not listed or prescribed under the Act may be deemed or permitted to act as a single unified custodian for their operations. This would greatly benefit healthcare organizations who wish to operate under a partnership model (such as the healthcare organizations in the Shared Information Management Services partnership[52] in Toronto) with a common goal of achieving health system integration.

---

[45] "Use" refers to any processing and treatment of data within an organization, whereas disclosure refers to the release of the information to third parties (outside of the originating organization, even in an EHR environment).

[46] For example, Ontario's PHIPA requires health information custodians to designate a "contact person" to facilitate and ensure compliance with the law. There is, thus, an existing model for accountability for the privacy and security of personal health information to be collected and distributed in an EHR in Ontario, at least from the perspective of the public knowing that custodians in the province must appoint an individual who they can contact to obtain information about information practices or acquire access to their own personal health information.

[47] Section 5(2) of Alberta's PIPA.

[48] Section 4(2) of B.C.'s PIPA requires organizations to be responsible for personal information under its control, including personal information that is not in the custody of the organization – which presumably extends to information held by its agents.

[49] Section 15(1)(b) of Ontario's PHIPA.

[50] Section 16(c) of Saskatchewan's HIPA.

[51] Sections 5, 6 and 7 of the Regulation made under Manitoba's PHIA. The pledge contains an acknowledgement that employees are bound by the trustee's policies and procedures and are aware of the consequences for breaching them

[52] SIMS is a partnership of 7 Greater Toronto Area healthcare organizations, including Bridgepoint Health Care, North York Community Access Centre, St. John's Rehabilitation Hospital, Toronto Community Care Access Centre, Toronto Rehabilitation Institute, University Health Network and West Park Health Centre. Its goal is to create a single information management collective to advance health

Should there be a single contact for an entire jurisdiction's implementation of the interoperable EHR? This would likely benefit patients but whether it would simplify administration of the interoperable EHR is unclear. If the answer is "yes," the appropriate means for implementing this in a given jurisdiction will require careful thought and planning.

Another information governance challenge will be to apply legal requirements drawn from the principles of the Model Code to a *pan-Canadian* interoperable EHR. For example, personal health information from Ontario might be accessed and then used by a healthcare provider in Newfoundland and Labrador. Unlike healthcare providers in Ontario, healthcare providers in Newfoundland and Labrador do not have a legal requirement to make available or explain data protection policies to patients. This type of jurisdictional inconsistency in privacy requirements will be problematic if it impedes the flow of personal health information from one jurisdiction to another. As noted earlier, the *Infoway* privacy and security conceptual architecture is built on the assumption that when data is disclosed from one jurisdiction to another via the interoperable EHR, the rules of the disclosing jurisdiction will apply. Exactly how this will be accomplished in practice has yet to be determined. Even if the recipient of a disclosure agreed to abide by the rules of the disclosing jurisdiction, how can a healthcare provider accessing the pan-Canadian interoperable EHR reasonably be expected to know the precise rules of his or her own jurisdiction and a dozen other jurisdictions as well?

Professional Codes of Conduct and other Privacy Guidelines

In addition to the existing legislative privacy schemes, national health professional associations have produced general codes of ethics, privacy guidelines and other resources to guide their members on issues of confidentiality and health information management. For example, the Canadian Medical Association (CMA) has developed a *Code of Ethics* for physicians and a *Health Information Privacy Code* that deals specifically with privacy, confidentiality and security of health information. Generally, these codes impose a duty to keep information confidential by preventing its disclosure unless authorized by the patient or where required by law.

With the advent of electronic medical systems and records, the need for security safeguards specific to information in electronic form has also been recognized. To that end, national organizations have created privacy and security guidelines for use in health care. For example, the Canadian Organization for Advancement in Computers in Health (COACH) has also created *Security and Privacy Guidelines for Health Information Systems* which focus on the security of health information in addition to privacy requirements for health information practices.[53] The CMA has also undertaken an e-health strategy in conjunction with its Health Information Technology Committee (HIT) which provides a number of recommended activities for introducing and implementing information technology in the healthcare sector. One of these included developing a privacy framework in order “to create a consistent confidentiality of personal health information environment across the country.”[54] There are a number of other resource documents published by the CMA, including “*Privacy Resources”* which link to

system integration and improve quality of care by enabling increased sharing of personal health information across the spectrum of care represented by its participating organizations.

53 See http://www.coachorg.com/default.asp?ID=439

54 See “*Shaping a Pan-Canadian e-health environment for Physicians and Patients*,” Discussion Paper, CMA HIT Committee, October 17, 2002; available at: http://www.cma.ca/multimedia/staticContent/HTML/N0/l2/HIT/pdf/e-health-discussion-paper.pdf

federal/provincial/territorial medical colleges and associations, "*Future Practice*" and "*IT Knowledge Centre*" which provide information on electronic communications, telemedicine, order entry and electronic records, as well as an online "*Privacy in Practice*" Handbook and a "*Privacy Wizard*" that allows members to create their own privacy policy.[55]

Also important are the privacy resources developed by various provincial regulatory health colleges and associations across Canada. In Alberta, the Medical Informatics Committee of the College of Physicians and Surgeons (CPSA) was created to:

1 Provide advice to the profession on the use of information management and information technology (IM/IT) in their medical practices, focusing on the ethical, legal, privacy, patient safety and quality improvement aspects;
2 Develop and coordinate CPSA input and leadership on IM/IT use in the healthcare system; and
3 Provide advice to CPSA staff about integrating IM/IT best practices into CPSA operations and programs.[56]

In response to the growing diversity of information management issues surrounding medical records, including electronic medical records held by physicians, and electronic health records held by regional health authorities and Alberta Health & Wellness, the CPSA is developing a set of comprehensive guidelines on data stewardship for the profession. In parallel with this effort, the College of Pharmacists in Alberta has prepared Guidelines on "*Offering Pharmacy Services via the Internet"* and the "*Pharmacists Guide to Applying the Health Information Act*."[57] This is in addition to sections 17-18 of the *Pharmaceutical Professional Regulation* (Alberta Regulation 322/94), which provides rules for electronic technology and requires an auxiliary system for electronic pharmacy records.

In British Columbia, the Medical Association and the College of Physicians and Surgeons of BC, in conjunction with the Information and Privacy Commissioner have created two helpful resources entitled "*Ten Principles for Protecting Patient and Client Information in Physician Practices*," and "*Ten Steps to Help Comply with PIPA*."[58] In addition, the BC Medical Association published a discussion paper outlining a vision for future health IT in BC, including 10 guiding principles for the development of an effective health information infrastructure.[59] The respective roles of these three BC institutions are mirrored in other Canadian jurisdictions. From an information governance perspective, the Medical Association represents the interests of physicians. The College is the regulatory body to which a physician could be reported in cases of allegations of breach of confidentiality and invasion of privacy and anyone can bring to the

---

55 See www.cma.ca.

56 College of Physicians and Surgeons of Alberta: Medical Informatics Committee, *Data Stewardship Framework*, Version 1.2, December 2006. Available at http://www.cpsa.ab.ca/publicationsresources/attachments_other/CPSA_Data_Stewardship_Framework.pdf.

57 See "*Offering Pharmacy Services via the Internet*," amended by the Council of the Alberta College of Pharmacists (May 2004) and "*Pharmacists Guide to Applying the Health Information Act* (February 2003 at: http://pharmacists.ab.ca/college.

58 See http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/TenPrinciples.pdf, and http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/tensteps.pdf.

59 See British Columbia Medical Association," *Getting It Right: Patient Centred Information Technology – A Discussion Paper by BC's Physicians*," January 2004, at: http://www.bcma.org/public/news_publications/publications/policy_papers/ITPaper/GettingITRight.htm

Information and Privacy Commissioner a privacy complaint against a healthcare organization or professional.

Lastly, other healthcare organizations not directly involved in providing treatment and care, but dealing with personal health information, such as research ethics boards, also draw guidance from a variety of privacy resources. See for example, the Canadian Institutes for Health Research (CIHR) "*Best Practices for Protecting Privacy in Health Research*,"[60] and the "*Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans*."[61] The latter document is a code of conduct for researchers, endorsed by the Medical Research Council of Canada, the National Science and Engineering Research Council, and the Social Sciences Research Council.

Valuable lessons can be drawn from this work by those responsible for the governance of the interoperable EHR. The challenge is to distil the wealth of material now available into a coherent set of principles that is specifically relevant to the interoperable EHR.

Oversight and Enforcement

The creation of penalties and offences within Canadian privacy legislation goes hand in hand with the powers of the Information and Privacy Commissioners.[62] Commissioners are independent Officers of the Legislature and not subject to political direction. Each Office is charged with the responsibility of overseeing information practices subject to legislation, which would also include privacy protective information practices for EHR implementations.

Generally, Information and Privacy Commissioners respond to health-related privacy complaints from the public by conducting investigations of the information practices of health information custodians and trustees, making recommendations, and/or issuing orders which in turn can be appealed to the courts. In some jurisdictions, the Commissioner has the power to conduct self-initiated reviews and to engage in pro-active monitoring for compliance via public education programs.

Public sector privacy laws also empower the Information and Privacy Commissioner as the oversight body to ensure compliance with privacy law. For example, the Commissioners in Nunavut and the Northwest Territories are empowered with investigatory powers to review, upon the request of an individual, any public healthcare body that has collected, used or disclosed personal information in contravention of the *Access to Information and Protection of Privacy Acts* and may issue recommendations based on his or her findings. Public bodies are also subject to prosecution for breaches of the Acts, including a maximum fine of $5,000.

The Commissioners and their staff recognize the importance of protecting personal health information. They can be valuable resources when establishing a privacy compliance regime. Consultation and collaboration with the Commissioners, along with other healthcare stakeholders, will form an important part of any future information governance solution for the handling of privacy and security issues in a pan-Canadian interoperable EHR.

---

60 See http://www.cihr-irsc.gc.ca/e/documents/pbp_sept2005_e.pdf.

61 See http://www.ncehr-cnerh.org/english/code_2/intro03.html.

62 In Manitoba, the oversight body is referred to as the Ombudsman who has broad powers under the PHIA, similar to that of Privacy Commissioners across Canada.

3.3 Implications for Information Governance

The privacy laws, privacy codes, and professional codes of practices discussed in the previous section have a direct impact on some of the twenty-one topics raised in chapter 2. In this section, we revisit these topics and examine the effect that these laws and codes may have on how certain issues are resolved.

Transborder and Cross-Jurisdictional Data Flows

Transborder and cross-jurisdictional data flows present potentially problematic governance issues in a pan-Canadian interoperable EHR because current Canadian privacy laws are not uniform and the rules for collecting, using and disclosing personal health information on the basis of consent vary among jurisdictions.

Healthcare organizations disclosing personal health information to another jurisdiction must do so in a manner that respects the legal requirements for consent in their own jurisdiction (i.e. the disclosing jurisdiction).[63] This means that a pan-Canadian interoperable EHR must have the functionality to record, where required by law, a patient's consent directives, including the withholding, withdrawal or revocation of consent. It also means that when the data is accepted by the custodian in the receiving jurisdiction(s), that the laws of the receiving jurisdiction(s) take effect.

Will Canadians understand and accept that, like the motor vehicles systems across Canada or the age of majority, variations exist in rules from jurisdiction to jurisdiction and that the rules that will apply are those of the province in which the data resides? What happens if the data resides in more than one jurisdiction? What constitutes a commercial transborder flow of data and thus one that could be subject to the provisions of PIPEDA? And does PIPEDA apply to the data only as it flows between jurisdictions or would such a flow be covered by data transfer agreements and the health and privacy legislation in the provinces involved in the transfer? These same questions apply to the current paper system, but in the pan-Canadian interoperable EHR environment, the volume of transfers can be expected to increase as shared service arrangements and approaches to the delivery of health care continue to evolve.

Harmonization of legislative privacy rules and consistent standards for data protection and cross-jurisdictional data flows would facilitate an interoperable EHR. But in its absence, perhaps, healthcare organizations involved in data transfers may wish to consider adopting the highest standard in place in order to facilitate such transfers and ensure compliance in all jurisdictions. This approach is consistent with international standards for data protection requirements for cross-border data flows, which seek to harmonize a range of differing national requirements to avoid conflict between national specifications.[64] This was first exemplified by the European Union (EU) Directive which established the parameters under which any data transfers from an EU member state to a non-EU member state could occur.

---

[63] Canada Health Infoway, *Electronic Health Record (EHR) Privacy and Security Requirements*, Reviewed with Jurisdictions and Providers, Revised February 7, 2005.

[64] See CSA standard CAN/CSA-Z22857-06 (ISO 22857:2004) Health informatics — Guidelines on data protection to facilitate transborder flows of personal health information.

The cross-border nature of electronic health care service delivery also poses additional legal challenges with respect to professional liability for healthcare providers, namely with respect to provincial/territorial licensure and credentialing. As noted earlier, although this paper does not deal with medico-legal liability issues with respect to health information, it is worth briefly noting what these issues mean for healthcare providers within the context of a pan-Canadian interoperable EHR. For example, currently there is no common approach to licensing and credentialing for health services. There may be a need to develop one for e-health services. Further issues may arise in relation to the lack of availability of cross-jurisdictional professional insurance. This could have the effect of precluding the provision of e-health services outside a healthcare custodian's jurisdiction since insurance coverage is based on the location of where care was provided to the patient. For example, the Canadian Medical Protective Association (CMPA) does not provide coverage for doctors who co-sign prescriptions without a prior doctor-patient relationship or for medical services provided to non-residents.[65]

Information Consent

Consent is a significant feature of Canadian privacy laws, as it is required for the collection, use or disclosure of personal health information, unless the relevant legislation permits or requires the collection, use or disclosure without consent. Each of the provincial health privacy statutes, as well as PIPEDA, have differing requirements for consent, the form of consent, (i.e. verbally or in writing), and the manner in which acceptable consent may be given. The differing consent regimes can best be illustrated by noting specific examples from various Canadian jurisdictions, such as Manitoba, Ontario, and Saskatchewan, which employ a non-consensual, implied and deemed consent model, respectively, for obtaining patient consent.

For example, Ontario's PHIPA uses an implied consent model for the collection, use or disclosure of personal health information.[66] Where consent is required by PHIPA, it must contain four elements as set out in section 18(1) of PHIPA. Specifically, consent must be: knowledgeable; relate to the information and must not be obtained through deception or coercion. Knowledgeable consent means that a patient must know the purpose for the collection, use or disclosure and know that he or she may provide or withhold consent.

In Manitoba's PHIA, consent is generally not required for the collection, use or disclosure of personal health information for healthcare and treatment purposes. For example, Section 15(1) permits collection without consent (but with notice). Section 21 permits the use of personal health information by trustees without consent for the purpose for which it was collected for authorized purposes listed under this statute or with an individual's consent for a purpose

[65] See CMPA "*Assistance in Internet and Cross-Border Prescribing to Non-Patients*," Information Sheet (March 2004) and "*Assistance in Legal Matters Arising from the Practice of Telehealth – General Principles*," Information Sheet (October 2003) at: http://www.cmpa-acpm.ca/cmpapd02/pub_index.cfm?LANG=E&URL=cmpa%5Fdocs%2Fenglish%2Fresource%5Ffiles%2Fadmin%5Fdocs%2Fcommon%2Fcom%5Findex%2De%2Ehtml

[66] The general rule for consent is found in section 29(1). This provision prohibits the collection, use or disclosure of personal health information by health information custodians without consent, unless PHIPA or another law permits or requires it. Where consent is required, it may be implied or express, except where the Act specifies it must be express. Section 18(3) provides that express consent is required for disclosures to non-health information custodians for any purpose or between health information custodians for purposes unrelated to providing or assisting in providing health care. In a pan-Canadian interoperable EHR this would mean, for example, that personal health information in Ontario requested by an employer or insurer would require the express consent of patients.

different from that for which it was initially collected. Similarly, section 22(1) authorizes disclosures without consent for the purposes listed in section 22(2) of the Act. While PHIPA in Ontario provides for knowledgeable consent, PHIA in Manitoba is silent on the type of consent required (i.e. knowledgeable or informed).

Saskatchewan's HIPA uses a deemed consent model, meaning that consent may be deemed between trustees who share personal health information for healthcare and treatment purposes. Section 6 of HIPA provides that, where consent is required for collection, use or disclosure of personal health information, it must relate to the purpose for which it was collected; be informed; be given voluntarily; and not be obtained through misrepresentation, fraud or deception. It is important to note that the element of "informed consent" in Saskatchewan is a different standard than knowledgeable consent in Ontario. To give informed consent, the Saskatchewan Act states that an individual must be provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure. This includes details such as who has access to the information, for what purposes, what security measures are in place to protect the information and what the risks and benefits are of refusing or consenting to the collection, use or disclosure.

From the above, we can see the challenges of recording a patient's consent in an interoperable EHR and in interpreting the meaning of the consent as data moves between jurisdictions.

Limiting Disclosure of Personal Health Information

Healthcare providers have a duty to disclose personal health information in a limited manner and to limit it to the minimum amount of information necessary for the identified purpose. This limitation principle is to be applied to employees and agents of health information custodians and trustees across Canada, including in Alberta,[67] British Columbia,[68] Manitoba,[69] Ontario[70] and Saskatchewan.[71]

The limitation principle in relation to uses and disclosures of personal health information can be illustrated by the privacy framework contained in Alberta's HIA. Custodians may use personal information without consent for the provision of health services or verification of eligibility to receive health services. Custodians may also disclose personal health information without patient consent to a person who is responsible for providing continuing treatment and care to the individual. Agreements with third parties must be entered into when using, storing or releasing such information outside of Alberta. In such cases, custodians are obligated to notify recipients (in writing) of both the purpose and statutory authority for this particular disclosure and keep a notation for 10 years (including the name of the person to whom the information was disclosed, the date, purpose and description of the information disclosed).

[67] Section 5(2) of Alberta's PIPA requires organizations to ensure its agents to comply with this Act.

[68] Section 4(2) requires organizations to be responsible for personal information under its control, including personal information that is not in the custody of the organization – which presumably extends to information held by its agents.

[69] Section 20(3) of Manitoba's PHIPA.

[70] Section 17(2) of Ontario's PHIPA sets out the general restriction for agents to only collect, use, disclose retain or dispose of personal health information on behalf of a custodian only if permitted to do so by that custodian and only if the custodian is permitted to collect, use or disclose the information, as the case may be (section 17(1)). This implies that agents are to adopt the information practices of the custodian.

[71] Section 23(2) of Saskatchewan's HIPA.

An individual's EHR may consist of hundreds of individual data fields. Complying with this limitation principle could be challenging if the EHR does not have the capability to select data fields for disclosure on a field-by-field basis. As noted in chapter 2, a clinically relevant and, at the same time, privacy-protective grouping of fields for the purposes of disclosure would greatly facilitate the limitation of personal health information disclosures. The satisfactory construction of such groupings would require an effective blend of clinical and information governance and take into consideration quality of care and patient safety concerns.

Technical Safeguards

Healthcare custodians are obligated to ensure that technical safeguards (referred to as security safeguard in Manitoba's PHIA and as security arrangements by the Personal Information Protections Acts in Alberta and BC) are in place to protect personal health information against theft, loss, and unauthorized use, disclosure, copying, modification or disposal.[72] But there does not appear to be any broad agreement in Canadian healthcare jurisdictions (or in most other jurisdictions) as to what constitutes adequate technical safeguards (or security safeguards or security arrangements).

This duty to use safeguards extends to custodians in Alberta who store or use health information in a jurisdiction outside of Alberta or disclose it to a person outside of Alberta. This involves ensuring health data is protected against threats or hazards to the security or integrity of the information or the loss, unauthorized use, disclosure or modification of the information. Section 60(1) of Alberta's HIA stipulates that safeguards must include appropriate measures for the security and confidentiality of records which must address the risk associated with electronic health records.

Section 16 of Saskatchewan's HIPA requires trustees to establish policies and maintain administrative, technical and physical safeguards with respect to personal health information. The Information and Privacy Commissioner in Saskatchewan has endorsed the *Guidelines for the Protection of Personal Health Information* produced by COACH as the standard for privacy and security protection by trustees in respect of section 16.[73]

In Manitoba, specific safeguards[74] for electronic records include implementing controls that (a) limit the persons who may use personal health information to those authorized to use it; (b) ensure that personal health information cannot be used unless identity and proper use is verified; and (c) include procedures to prevent the unauthorized interception of information transferred by electronic means. Trustees in Manitoba must also be able to produce an electronic record of successful or unsuccessful attempts to gain access to records, and attempts to add to, delete or modify that information; record every transmission of personal health information maintained on the system; and review the electronic records regularly to detect any security breaches. [75]

---

[72] For example, see section 34 in each the Alberta and B.C's PIPA; section 12(1) in Ontario's PHIPA; Section 3(c) of the Regulation made under Manitoba's PHIA and Section 16(b)(i)-(iii) of Saskatchewan's HIPA.

[73] See www.coachorg.com

[74] Section 18(1) of Manitoba's PHIA.

[75] Section 4(1) and (2) of the Regulation made under Manitoba's PHIA.

As mentioned in section 2.4, questions about the acceptability of residual security risks identified in EHR systems have remained largely unanswered. The frequency with which Canadian healthcare organizations are conducting TRAs and PIAs today varies. In Ontario, it is a requirement of the Ontario Ministry of Government Services that a PIA be conducted where changes to the management of personal information held by Ministry programs "may affect client privacy."[76] PHIPA also requires that PIAs be conducted by "health information network providers." However, Alberta's HIA requires health information custodians to prepare a PIA for submission to Alberta's Information and Privacy Commissioner before implementing any new practices or changing existing practices or systems.[77]

Infoway's *Electronic Health Record (EHR) Privacy and Security Requirements*[78] provide a baseline for security safeguards for the interoperable EHR.

Security Incident Handling and Privacy Breach Notification

Chapter 2 noted that guidelines are required on how to handle privacy breaches and when and how patients are to be notified of a privacy breach. However, it is important to note that responsibilities and sanctions related to privacy breaches are not only being set in legislation, but by administrative rulings as well and that these too will have an impact on health information governance. For example, in a recent ruling (September 2006), the Ontario Information and Privacy Commissioner (IPC) ordered The Ottawa Hospital to review and revise its practices, procedures and protocols relating to patient information and privacy as a result of her investigation into a privacy complaint. The affected patient in this case complained to the IPC that, during and after her treatment at The Ottawa Hospital as an in-patient, her personal health information was illegally accessed on 10 known occasions by two hospital employees. Despite the privacy office being notified of the breach, unauthorized access to the complainant's electronic record continued for at least three weeks. The IPC ordered the hospital to implement a protocol as part of this review to ensure that reasonable and immediate steps be taken upon being notified of an actual or potential breach of privacy.[79]

Professional regulatory tribunals have also sent clear messages to healthcare providers that privacy breaches will not go unpunished. For example, the College of Pharmacists in British Columbia disciplined and fined five pharmacists for inappropriately accessing the medication records of colleagues, relatives and friends contained in an electronic pharmaceutical information system called BC PharmaNet.[80] Those responsible for the information governance of the interoperable EHR will need to consider the rulings of such tribunals and the precedents that they set.

---

[76] The Ontario Ministry of Government Services' *Privacy Impact Assessment Guidelines* are designed to ensure that Ministries of the Government of Ontario meet their privacy obligations under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

[77] Examples include transferring paper-based records to digital format or integrating two existing information systems) to ensure that the public is fully informed about how their personal health information will be protected in new electronic environments.

[78] Canada Health Infoway. *Electronic Health Record (EHR) Privacy and Security Requirements, version 1.1, 2005*.

[79] See IPC Order HO-002 available at http://www.ipc.on.ca/docs/HO-002.pdf.

[80] See discussion paper entitled "*Getting It Right: Patient Centred Information Technology, A Discussion Paper by BC's Physicians*," January 2004, available online at: http://torch.cs.dal.ca/~smit/publications/public_opinion_electronic_health_records_solutions.pdf

The "Need-to-Know" Principle

Canadian privacy legislation requires that access controls support the "need-to-know" principle, an idea that is easy to understand in theory but can be challenging to implement in practice. For example, as noted in section 2.6, one particularly challenging aspect of expanding existing systems of access control from physician or hospital-based systems to the EHR Infostructure will be to effectively establish user roles for EHR Infostructure users.[81] Nevertheless, user roles can be an effective means of instantiating the "need-to-know" principle in the architecture of the EHR Infostructure.

A healthcare concept closely related to the "need to know" principle is the "circle of care," a notion that is not defined in any specific privacy law but that commentators, including the Ontario and federal Privacy Commissioners, have used for illustrative purposes when referring to those health care providers involved in providing direct treatment and care to their patients.[82] An important qualification is that information sharing has to be "reasonably necessary" for the provision of health care. The "circle of care" is difficult to define for a pan-Canadian interoperable EHR. It can differ for each episode of care. It can differ depending on whether the patient is being treated for a broken leg or for cancer. There is also the question as to whether the circle of care encompasses the same types of healthcare providers in all provinces. Such questions need to be answered before the circle-of-care concept can be usefully applied to the information governance of the interoperable EHR.

---

81 Among the types of access control discussed in *Infoway's* Privacy and Security Conceptual Architecture, role-based access control is especially important as a component of the overall EHRi access control strategy. This form of access control assigns each user to one or more user roles. Each user role is then mapped to one or more EHRi access privileges. These access privileges consist of sets of data fields and associated access modes (read only, update, etc.), and sets of EHRi capabilities (patient search, etc.). By judiciously defining a limited number of roles and mapping them to a manageable set of access privileges, administrators can quickly assign each user just those access privileges that are needed by someone in the user's role. The alternative—assigning privileges to users on an ad hoc, user-by-user basis—has historically been shown to be unwieldy, error prone, and insecure.

82 See Ontario Hospital Association, *Hospital Privacy Toolkit*, pp. 51-53.

4. INFORMATION GOVERNANCE STRUCTURES IN CANADIAN HEALTH CARE

4.1 Introduction

Current leaders of healthcare organizations generally do not need to be persuaded of the importance of ensuring appropriate information governance structures and processes for handling privacy and security issues. They are already keenly aware that they will be held responsible by Information and Privacy Commissioners, politicians, public servants, and, ultimately, the courts for serious breaches of privacy or security. As a result, many healthcare organizations have already established information governance structures and processes with a chain of accountability for handling privacy breaches and security incidents. These information governance structures exist at several levels in Canadian health care:

- In primary care practices;
- In healthcare institutions such as hospitals;
- In regional health authorities;
- In government-funded agencies that deal with a specific disease, such as cancer, mental health or HIV/AIDS;
- In provincial information infostructures, such as registries or data warehouses; and
- In healthcare organizations with large holdings of personal health information (referred to as domain repositories by *Infoway*).

This chapter describes how information governance is already being carried out among the diverse health information custodians, trustees and institutions that make up health care in Canada. As with chapters 2 and 3, the discussion that follows is intended to be illustrative, not exhaustive.

The laws and regulations described in the previous chapter shape the way information governance is structured and there is considerable variety in the types, size and complexity of information governance structures within which healthcare providers and healthcare organizations operate in Canada. For example, a healthcare institution's board of directors may be established by an act that outlines the general rules for the existence and operation of a specific healthcare organization or facility. The privacy and security obligations for that organization or facility typically are contained in separate privacy legislation which applies to the collection, use and disclosure of personal health information in the jurisdiction within which the organization or facility operates.

In other cases, legislation may provide for a specific corporate governance structure. For example, the *Centre for Health Information Act* (CHIA) in Newfoundland and Labrador sets out the objects for the Centre for Health Information, as described in section 3.2. The CHIA establishes the Centre's internal corporate governance structure by providing rules for the appointment of directors, terms of office, frequency of general meetings, audits, funding and other financial matters. Regardless of the type of information governance structure in place, healthcare providers and administrators want assurances that the appropriate privacy and security management controls are in place.[83]

[83] See Ontario Information and Privacy Commissioner, "*Privacy and Boards of Directors: What You Don't Know Can Hurt You*," (November, 2003), available at http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=14757&U_ID=0

4.2 Information Governance in Primary Care Practices

In solo physician practices, a family physician will typically act as his or her own privacy officer. Some physicians, however, have sought to achieve economies of scale in the computerization of their offices and the management of personal health information. For example, Alberta's Physician Office System Program (POSP) was created in early 2001 through an agreement between the government of Alberta and the Alberta Medical Association. Physicians receive funding through POSP to automate their paper-based office with electronic medical record (EMR) systems having the capability to link to, or integrate with, a variety of provincial information systems. Since the program's inception in 2001, the funding models which form the foundation of the program have evolved, as has the program governance structure.

POSP currently operates under a tri-partite governance agreement between Alberta Health and Wellness, the Alberta Medical Association and Alberta's nine Regional Health Authorities. These organizations all appoint representatives to the Physician Office System Program Committee who, in turn, make operational decisions related to the program. POSP is supported by a program management office.

POSP does not assume information governance responsibilities on behalf of health information custodians[84] nor does POSP assume custody or control of health information. Rather, POSP's role in the information governance process is to develop relevant program policy related to information governance and support custodians in responding to issues related to information governance within their clinic environment. POSP has developed several innovative methods of addressing these concerns. These include:

- Requiring physicians to develop a strategy which addresses critical issues of information governance when a physician leaves the practice as part of the Readiness Assessment;
- Leading technical work on the "Transfer of Patient Data" and "Conversion of Patient Data" projects which provides exiting custodians with the flexibility to migrate their patient data from one EMR application to another;
- Ensuring that approved EMR applications possess the technical functionality to support pre-determined information governance practices through the Vendor Conformance and Usability Requirements (VCUR) process; and
- Assisting custodians transitioning to an EMR environment to complete a Privacy Impact Assessment as required under Alberta's *Health Information Act* through their Change Management services.

The latter activity has resulted in several positive information governance activities, such as the appointment of a responsible affiliate, development of policies and procedures related to information management and assessment of the unique risks associated with the transition to an EMR in a given clinic environment. Completion of a PIA and submission of that document to the Office of the Information and Privacy Commissioner of Alberta is a condition of funding for POSP.

---

[84] As defined in section 1(1)(f) of Alberta's HIA.

Other provinces are embarking on similar physician automation initiatives, including the Ontario MD program[85] and the BC Physician Information Technology Office (PITO) program.[86] These initiatives serve the same purpose as POSP in that they subsidize physicians' implementation of pre-qualified or certified EMR systems. However, the POSP program is currently the most broadly adopted program, with more than 3,369 or 61 per cent of Alberta physicians enrolled in the program as of July 2006.[87]

4.3 Information Governance of Hospitals and Other Public Healthcare Institutions

University Health Network (UHN) is one of Canada's largest teaching hospitals, located in downtown Toronto, Ontario. It comprises three sites — Toronto General Hospital, Toronto Western Hospital, and Princess Margaret Hospital — and is affiliated with the University of Toronto. In delivering healthcare services to approximately 30,000 in-patients across its sites, UHN generates records on over five million patients. In its designated role as a health information custodian[88] under Ontario's PHIPA, UHN must keep all personal health information under its custody and control, in a confidential and secure manner.

At UHN, the legal framework for privacy is primarily determined by PHIPA. Ultimate accountability for UHN's compliance rests with the Board of Governors and the hospital's President and Chief Executive Officer (CEO). The information governance practices are overseen by the UHN Privacy Office under the direction of the Privacy Manager who reports indirectly to the hospital's xecutive Vice-President and Chief Information Officer. The Executive Vice-President and Chief Information Officer report major privacy breaches and security incidents to the President and CEO and to the hospital's Board of Governor (where appropriate). Staff are also required to report privacy breaches to the UHN Privacy Manager and to the Patient Relations Office in cases where patient privacy is affected.

UHN's Privacy Policy is based on the CSA Model Code and discusses each principle individually as it relates to personal health information at UHN. The policy was approved by the hospital's Board in 2002. The policy is made available publicly on the UHN website.[89] Furthermore, UHN has implemented practices to give effect to this policy that include specific internal procedures to protect personal health information, in accordance with Ontario's *PHIPA*. Other corporate governance mechanisms in place at UHN include contractual agreements (i.e., confidentiality agreements signed by all agents of UHN, including the organizations in the SIMS Partnership) for ensuring privacy compliance.

Ontario's *Public Hospitals Act* and its accompanying Regulation[90] also impacts UHN in terms of its internal operations, administrative practices, and its governance structure. For example, UHN — and all other public hospitals in Ontario — are required to have in place a board of directors and various committees as per the regulatory requirements set out under Regulation 965 made under the Act. A hospital board typically uses committees in areas that require key decision-

85 http://www.ontariomdtsp.ca/

86 http://www.health.gov.bc.ca/msp/legislation/bcmaagree_faqs_pito.html#1

87 http://www.posp.ab.ca/news/03-22-2006.asp

88 As defined in section 3(1)4(i) of Ontario's PHIPA.

89 See http://www.uhn.ca/patient/privacy/docs/uhn_privacy_policy.pdf

90 Hospital Management, R.R.O. 1990, Ontario Regulation 965, Amended to Ontario Regulation 204/06.

making or approvals and this can include a privacy and security committee in response to *PHIPA*'s legislative requirements. It is not uncommon for hospital boards to receive at least annual briefings on privacy and security, with a standing committee of the board, such as a risk management committee or quality committee, receiving briefings more often.[91]

This regulation further prescribes detailed rules that the hospital board and various committee members must follow. Specifically, the overall management and administration of UHN is required to be set out in hospital by-laws (i.e., the internal rules and operating procedures), including, for example, a description of the functions and responsibilities of the officers of the board and procedures for their appointment. When discharging its responsibilities, the hospital board must also provide leadership, with specific responsibility to ensure legal compliance with other statutes of general application, which includes Ontario's *PHIPA*.

4.4 Information Governance in Regional Health Authorities

As is the case in several provinces, BC's healthcare system is delivered through health authorities. The Vancouver Coastal Health (VCH) authority is responsible for providing five different health services (acute and hospital care, home and community care, mental health and addictions services, and public health) across 550 sites in BC. VCH draws primarily on the *Freedom of Information and Protection of Privacy Act* for its information governance processes. It is also subject to BC's *Regional Health Authorities Act* which sets out the conditions under which regional health boards are designated and the RHAs are incorporated and created, as well as the duties and responsibilities of these boards. The primary responsibilities of a regional health board are to develop and implement a regional health plan, to develop policies, set priorities, prepare and submit budgets to the health minister and allocate resources for the delivery of health services under the regional health plan and to develop and implement regional standards for health care delivery in the region.

VCH has a signed performance agreement with the Ministry of Health which defines expectations, performance deliverables and service requirements for which VCH will be held accountable. To carry out these responsibilities, the board has established three standing board committees, each of which operates under terms of reference outlining its authority and responsibility. For example, the Governance and HR Committee focuses on ongoing director development and succession planning. This Committee works with the Board to put in place essential elements such as a Code of Conduct and Conflict of Interest Guidelines.

Accountability also extends to health information. In May 2006, VCH created an information governance Steering Committee and Working Group with respect to health information privacy governance. The Steering Committee includes the Chief Financial Officer, Chief Information Officer, Vice-President of Employee Engagement, Vice-President of Medical Clinical Quality and Safety, Legal Counsel and Director of Client Relations and Risk Management. This Committee meets on an as-needed basis to discuss privacy and information security risk management issues and compliance measures, among other governance issues. The Working Group consists of 25 members. It was created in tandem with the Steering Committee to help vet policies, change management processes and assist with the shift to an electronic health record environment.

[91] The Board of the Canadian Institute for Health Information (CIHI) is a pioneer in this regard having created a formal Privacy and Data Protection Committee of its Board.

The privacy and information governance structure at VCH is based upon a centralized model with uniform application across all healthcare providers and all affected organizations across the region. For example, VCH is governed by one common Regional Information Privacy and Confidentiality Policy with respect to its personal information privacy practices and has created one centralized Information Privacy Office for the entire region. The investigation and containment of a privacy breach at any facility within the region or involving any healthcare provider is co-ordinated centrally through the Information Privacy Office. FOI coordination is assigned centrally to a coordinator in the Communications group and access to health records is dealt with through the health records department of the facility where the patient received care. A new Security Services group was recently established within IMIS for protection of system and information assets. The Information Privacy Office at VCH is currently supported by one Regional Manager and two Privacy Advisors, supplemented periodically by contract project resources.

4.5 Information Governance of Government-Funded Health Agencies

The Canadian healthcare system includes dozens of provincially funded agencies with mandates to further the prevention and treatment of specific diseases. In this section, we examine the information governance structure of one such provincial health agency.

Cancer Care Ontario (CCO) is a provincially funded planning and research organization that advises the Ontario government on all aspects of provincial cancer care. It also provides planning and management information to healthcare providers and decision-makers and promotes better cancer care. It is accountable to the Minister of Health and Long-Term Care in exercising its mandate. Its mandate and relationship with the Ministry are outlined in a Memorandum of Understanding (MOU).

In fulfilling its mandate, CCO collects personal health information for planning and management purposes from healthcare providers and institutions, such as hospitals, that are directly involved in treatment and care. It also collects personal health information from other sources, such as the Canadian Institute for Health Information (CIHI) and Statistics Canada. CCO has authority to collect, use and disclose such information for the purpose of health system planning and management, without patient consent, under the authority of section 45 of PHIPA. This information is retained in such large databases at CCO as the Ontario Cancer Registry and the newly created Wait Times Information System (WTIS), which CCO will operate until March 2008.

As a prescribed entity under Section 45 of *PHIPA*, CCO is subject to oversight by the Information and Privacy Commissioner/Ontario (IPC) and must have its information practices reviewed and approved every three years by the Privacy Commissioner's Office. The IPC approved CCO's information practices in November 2005.

Although not specifically required to do so under PHIPA, CCO has appointed a Chief Privacy Officer (CPO) who reports directly to CCO's President and CEO and oversees CCO's Privacy Compliance Program. It has also established a core Privacy Team that includes Privacy Leads who are responsible for ensuring privacy policies are adhered to and Data Stewards who ensure data holdings are managed in accordance with their identified purposes. It also has a security team which includes the Chief Information Officer, Director of Information Technology and a Systems Security Specialist.

Key components of CCO's Privacy Compliance Program include CCO's Privacy Policies and related procedures, mandatory employee privacy and security orientation and training program, and privacy impact assessments on CCO data holdings and new proposals. The CPO is supported in carrying out the Privacy Compliance Program by individuals and committees with specific privacy and security-related responsibilities. For example, to support the WTIS, CCO has established and appointed the Wait Time Information Office (WTIO) to be responsible for administering this system and reporting wait times information on CCO's behalf. The WTIO Privacy Lead is responsible for the day-to-day operation and privacy processes within the WTIO and reports to the CPO at CCO. Responsibility for general PHIPA compliance on behalf of the WTIO rests with the WTIS Privacy Lead through WTIS specific data protection policies.

To ensure that end-users connected to the WTIS understand their custodial responsibilities with respect to the system, hospitals must sign acceptable use agreements. These agreements clarify the specific privacy and security responsibilities that hospital sites must uphold when accessing personal health information via the WTIS.

Lastly, CCO and the Ministry have entered into a data-sharing agreement to govern how personal health information by the WTIO will be handled. It confirms, among other things, WTIO's responsibility to maintain all personal health information it receives from CCO in accordance with the privacy rules set out in PHIPA and other applicable legislation. CCO also has agreements with other section 45 entities and agents to cover the collection, use and disclosure of personal health information.

4.6 Information Governance of Provincial Health Information Infostructures

Alberta, BC, Newfoundland and Labrador, Ontario and Saskatchewan are among the provinces that have a coordinated, province-wide health information infostructure. This section describes the information governance structure of three of these infostructures.

Newfoundland and Labrador Centre for Health Information[92]

The Newfoundland and Labrador Centre for Health Information was established to provide quality information to health professionals, the public, and health system decision makers. Through collaboration with the health system, the Centre supports the development of standards, maintains key provincial health databases, prepares and distributes health reports, and supports and carries out applied health research and evaluations. The Centre's mandate also includes the development of a confidential and secure health information network to serve as the foundation for the provincial EHR.

Besides supporting the health information needs of its stakeholders, the Centre provides a return on the provincial government's investment by attracting external funding for health information technology projects and applied health research. The Centre is building capacity for EHR development in the local technology industry and applied health research skills in health researchers. In 2004, the Centre began operating the first provincial client registry designed and implemented specifically for the EHR. The Centre also makes significant contributions to data

[92] Newfoundland and Labrador Centre for Health Information, *Preliminary Privacy Impact Assessment: Newfoundland and Labrador Interoperable Electronic Health Record* (Confidential Draft), October 18, 2006.

standards development and dissemination, applied health research and the evaluation of health information systems.

The Centre was established by the provincial government in 1996 and is governed by a Board of Management appointed by the Minister of Health and Community Services, and managed by a Chief Executive Officer. It functions under the Board of Trustees of a regional health authority (Eastern Health), pending proclamation of the *Centre for Health Information Act,* which will establish the Centre as a provincial government agency under the Corporations Act (proclamation is expected in 2007). The Centre will continue to report to the Minister of Health and Community Services.

The Centre is divided into four divisions; Health Information Network, Data Quality and Standards, Research and Evaluation, and Privacy and Corporate Services. It currently employs 50 full and part-time staff. The majority of staff members are located in St. John's.

Additional information concerning the Centre is available on its website at: http://www.nlchi.nf.ca/

Ontario Smart Systems for Health Agency

Ontario's Smart Systems for Health Agency (SSHA) was established to provide a secure province-wide IT infrastructure for the collection, transmission, storage and exchange of health information. It was created pursuant to a regulation made under the *Development Corporations Act*[93]*,* which establishes the legal existence, structure and mandate of SSHA. It is ultimately accountable to the Ontario Minister of Health and Long-Term Care.

The overall goal of SSHA is to create a patient information sharing network in order to connect various types of healthcare providers and organizations across the province, as mandated by the provincial government. SSHA's mandate is also determined pursuant to a Memorandum of Understanding between SSHA and the Ministry. When fully operational, SSHA will connect more than 150,000 healthcare providers across 24,000 sites throughout Ontario.[94]

The agency's mandate is overseen by a board of directors appointed by the provincial government. Furthermore, SSHA is legally required to submit annual reports to the Minister that must include a general description of every instance of unauthorized access to personal health information within the Agency's infrastructure, as per section 10(2) of SSHA's governing regulation.

In addition, the network services provided by SSHA qualify the organization to comply with the definition of a "health information network provider" under Ontario's PHIPA Regulation. Specifically, section 6(3) defines a health information network provider as a person who provides services to two or more health information custodians to enable these custodians to use electronic means to share personal health information.[95] In providing network services to healthcare providers and organizations, SSHA must fulfil a number of prescribed requirements,

[93] Ontario Regulation 43/02.

[94] See http://www.thinksmart.ca/about/index.html.

[95] Section 6(2) of Ontario Regulation 329/04 made under PHIPA defines a health information network provider as "person who provides services to two or more health information custodians to enable these custodians to use electronic means to share personal health information." Section 6(3) of PHIPA prescribes certain duties that health information network providers must undertake.

including notifying every custodian at the first reasonable opportunity of any breach relating to the unauthorized access, use, disclosure, or disposal of personal health information by SSHA. Healthcare providers and organizations which utilize SSHA infrastructure services are required by SSHA to incorporate privacy, security and acceptable use requirements into a contract or MOU that sets out terms and conditions under which SSHA will provide its services.

Alberta Data Stewardship Committee

Another approach to information governance at the provincial level is that taken by Alberta through its Data Stewardship Committee. Alberta Health and Wellness established the Electronic Health Record Data Stewardship Committee in 2003 *via* Ministerial Order. While the composition and reporting structure of the Data Stewardship Committee (DSC) have varied since its inception, membership of the DSC has consistently included representatives of the Department, regional health authorities, health professional associations (Alberta Medical Association and Pharmacists Association of Alberta), health professional regulatory bodies (College of Physicians and Surgeons of Alberta and the Alberta College of Pharmacists) and members of the general public. Membership has been limited to approximately 12 members at any given time. The DSC currently reports directly to the Minister of Alberta Health and Wellness and is mandated to define and approve the rules related to EHR data, access, use and disclosure.[96]

The legislative environment in Alberta is such that Alberta Health and Wellness (AHW) acts as an information manager[97] for custodians participating in the EHR. As an information manager, AHW provides the infostructure for the operation of the provincial EHR and enters into agreements regarding its development on behalf of all participating custodians. This information management relationship between AHW and custodians is laid out in a master Data Sharing Agreement (DSA) that binds participants to an Information Exchange Protocol (IEP), which in turn describes the purposes for which personal health information in the EHR may be used. It also expressly limits secondary uses of data (i.e., research cannot be conducted using data from the EHR) and binds custodians to certain obligations, such as ensuring any POS system they are connecting to the EHR has adequate safeguards. The Data Sharing Agreement and IEP are the primary vehicles through which the Alberta EHR is governed. As the Information Manager for the EHR, AHW manages the EHR in accordance with the terms of these agreements. In addition, all custodians are bound by the terms of the DSA and IEP prior to being granted EHR access.

The terms of the Data Sharing Agreement and IEP grant the DSC the authority to amend the terms of the data-sharing agreement and information exchange protocols on behalf of participating custodians at any time. As such, this group exerts considerable influence over the development and management of the provincial EHR.

4.7 Information Governance of Major Public Holdings of Personal Health Information (Domain Repositories)

The interoperable pan-Canadian EHR will ultimately derive much of its access to personal health information from major domain repositories, such as the Alberta Pharmacy Information

[95] This footnote was included in error.
[97] The term “information manager” is defined in section 1(1) of Alberta's HIA.

Network, BC Pharmanet, the Ontario Laboratory Information System (OLIS), and others. The oldest, and one of the largest of these domain repositories, is PharmaNet.

PharmaNet, BC's provincial drug information system, was implemented by the BC Ministry of Health in September 1995. PharmaNet connects community pharmacies, outpatient hospital dispensaries, and emergency rooms to a common health information infostructure. Some hospitals and primary care physician offices in BC are also now connected to PharmaNet. Every individual who has a prescription filled in BC — both residents and non-residents — is registered in PharmaNet. The PharmaNet database contains a 14-month history of all medications dispensed, all adverse drug reactions recorded, and relevant clinical conditions for each individual in the system.[98]

PharmaNet is created under, and functions in compliance with, the *Pharmacists, Pharmacy Operations and Drug Scheduling Act* (PPODSA). Under the PPODSA, the BC Minister of Health is ultimately responsible for managing PharmaNet.[99] However, the BC College of Pharmacists has custodial (i.e., information governance) responsibilities for the information in PharmaNet and has the authority to discipline pharmacists who access personal health information for unauthorized purposes. This has occurred on several occasions.[100]

Section 38 of the PPODSA creates a "PharmaNet Committee" to manage the disclosure of personal health information and general drug information.[101] The Act requires that the PharmaNet Committee not consist of more than 10 members and specifies requirements for its composition — namely, that it must consist of three persons nominated by the minister, one person nominated by the council of the College of Physicians and Surgeons of British Columbia, and one person nominated by the Dean of the Faculty of Pharmaceutical Sciences at the University of British Columbia.[102] The PharmaNet Committee serves as the gatekeeper of the personal health information in PharmaNet for secondary purposes,[103] including research, quality improvement/assurance, and fraud investigation and monitoring.[104]

98 British Columbia Medical Association, *Getting it Right: Patient Centred Information Technology,* January 2004; available at: www.bcma.org.

99 Section 37(2), *Pharmacists, Pharmacy Operations and Drug Scheduling Act*, RSBC 1996, Chapter 363.

100 David Loukidelis, Information and Privacy Commissioner/British Columbia, *Health Information Privacy: The British Columbia Experience,* Canadian Institute Conference – Toronto, June 19, 2001.

101 Section 38, *Pharmacists, Pharmacy Operations and Drug Scheduling Act*, RSBC 1996, Chapter 363.

102 Section 38 (2), *Pharmacists, Pharmacy Operations and Drug Scheduling Act*, RSBC 1996, Chapter 363.

103 A PharmaNet Committee *Application for Release of Information form* is available at: http://www.bcpharmacists.org/pharmanet/agreements/pdf/PharmaNet_Committee_Application_for_Release_of_Information.pdf

104 Section 39 (4), *Pharmacists, Pharmacy Operations and Drug Scheduling Act*, RSBC 1996, Chapter 363.

5. INFORMATION GOVERNANCE MECHANISMS IN CANADIAN HEALTH CARE

Health information custodians and trustees can rely upon a variety of mechanisms or established processes to help them comply with legislative privacy and security rules and requirements. For example, although it is not a legal requirement contained in any of the legislation discussed in Chapter 3, a privacy or security team can be an effective mechanism for dealing effectively with privacy and security concerns.[105] Many healthcare organizations have established such teams as a way of detecting data protection problems, fostering privacy-sensitive and security-sensitive organizational cultures, and helping ensure compliance with applicable laws and institutional policies and procedures.

There are also tools available such as the ACIET *Pan-Canadian Health Information Privacy and Confidentiality Framework* [106] and the College of Physicians and Surgeons of Alberta: Medical Informatics Committee's *Data Stewardship Framework*[107], that provide guidance on common and consistent statutory provisions as well as information governance requirements and mechanisms..

This chapter describes information governance mechanisms currently in use in the Canadian healthcare system which could be extended to the interoperable EHR context. Because these mechanisms tend to be most effective when they are applied as a suite of data protection solutions, the discussion does not apply them to the specific information governance issues introduced in Chapter 2.

5.1 Privacy Policies, Security Policies, and Statements of Information Practices

Statement of Information Practices

To inform patients of the purpose for the collection of their personal information, and how the information will be used and protected, healthcare providers and organizations can post notices explaining their information practices. Notices may be posted in a variety of locations, including on the Internet, on an office wall, in a pamphlet available in a waiting room, in consent to treatment forms, or in a registration form that is given to new patients at the time of initial enrolment.[108] While the notice can include or make reference to the organization's privacy

---

[105] See for example, ISO 17799: *Information Technology – Code of Practice for Information Security Management* which recommends that "management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities." (page 13).

[106] Advisory Committee on Information and Emerging Technologies (ACIET), *Pan-Canadian Health Information Privacy and Confidentiality Framework*, Ottawa: Health and the Information Highway Division, Health Canada, January 2005. Available at http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html.

[107] College of Physicians and Surgeons of Alberta: Medical Informatics Committee, *Data Stewardship Framework*, Version 1.2, December 2006. Available at http://www.cpsa.ab.ca/publicationsresources/attachments_other/CPSA_Data_Stewardship_Framework.pdf.

[108] Some suggested methods of meeting this requirement include the use of visible brochures, posters, notices posted on walls, and verbal explanations. See Ontario IPC, *Frequently Asked Questions Health Information Protection Act* (updated Oct. 22, 2004). The OHA, *Hospital Privacy Toolkit*, p. 11 has a sample written statement of information practices. These should contain sufficient detail to satisfy the privacy fundamentalists in the population. On the other hand, one page will likely satisfy the

policy, an organization's security policy is not usually made public and so only general statements about security are typically made in the statement of information practices.[109] The goal is to give information about privacy protection to those who are interested and to explain to patients what type of safeguards are in place to protect personal health information from unauthorized collection, use, disclosure, modification, disposal and access.

Privacy Policy

Most large healthcare organizations, and many small ones, have a written privacy policy. Such policies are often based upon the principled approach used in the CSA Model Code, which has been formally incorporated as Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[110] Healthcare organizations often make a copy of their privacy policy, or an abbreviated summary, available on the organization's website.

Security Policy

Security policies are an essential component of the security controls described in the ISO 17799 security standard (*Information Technology – Code of Practice for Information Security Management)* that has been adopted for use in health care by the BC Health Information Standards Council. The Ontario Health Information Standards Council has also endorsed the portion of this standard that recommends the use of written security policies. A written security policy was also a requirement of the *Infoway* Privacy and Security Requirements (security requirement 2).

Security policies typically need to cover subjects such as: security organization and responsibility, management of information assets, human resources security, physical security, communications security and operations management, access control, systems development, acquisition and maintenance, incident handling, business continuity management, and compliance.

5.2 Other Policies Related to Information Governance

A privacy policy and a security policy will generally include or be supplemented by:

- A confidentiality policy with an accompanying confidentiality agreement;
- A system access policy;
- A policy on acceptable use of information technology resources;
- A policy on access to personal health information for research, education and quality assurance purposes;

---

bulk of the population, who are either privacy pragmatists or who claim not to be concerned about their privacy interests.

[109] For an example of such an information statement for hospital patients, see Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*, appendix 3.

[110] The BC government has a “fill in the blanks” form to use to develop a privacy policy for BC PIPA; see PIPA Implementation Tool 8 at http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/Pipa_Tool_8.htm. For an example of such a privacy policy for an Ontario hospital, see Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*, appendix 1.

- A policy to address requests to access and correct personal health information in patient records; and
- A policy on retention and destruction of health records.

There are plenty of existing models for such policies to be found among Canada's provinces and territories which can then be adapted to fit local needs and statutory requirements. The interlinked websites of the various Information and Privacy commissioners across the country are excellent sources of guidance.[111]

5.3 Privacy Officers and Privacy Teams

Although health information custodians are ultimately responsible for the personal information in their custody or control, the tasks involved in ensuring privacy protection can be delegated to a staff person designated as the (Chief) Privacy Officer, who then carries out these tasks to promote compliance, particularly in large healthcare organizations.[112]

The most important tasks of a Privacy Officer in a healthcare setting are to understand the requirements of applicable legislation, to provide ongoing privacy and security training, and to answer questions about data protection and security from staff, patients and the public about the various data protection policies of the healthcare institution or practice.[113] Privacy Officers play a key role in investigating suspected problems and managing problems which arise. They should also be part of the business team responsible for policy, process and technology decisions to ensure that privacy and confidentiality are considered and privacy enhancing solutions are adopted wherever possible.

5.4 Information Security Officers and Security Teams

In many organizations, the role of the (Chief) Information Security Officer is also essential for achieving robust data protection and security practices. Information security officers have responsibility for information security management and information security technology. They are normally assisted by teams that, in large healthcare organizations, cross organizational boundaries. Privacy and security officers work closely together.

5.5 Privacy Awareness Training

Privacy awareness training which includes all related policies and procedures appropriate to the individual's role ensures that everyone handling personal health information understands the sensitive nature of the information involved. In the case of the interoperable EHR, they need to understand the powerful nature of the systems they are using, the responsibilities associated

[111] The website of the Privacy Commissioner of Canada has a complete list of the names, addresses, and websites of the provincial and territorial commissioners as well as government sites. See http://www.privcom.gc.ca/information/comms_e.asp

[112] BC, PIPA, s. 4. See PIPA Implementation Tool 3: "What is a Privacy Officer?" at http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/PIPA_Tool_3.htm. See also "New privacy legislation now in force: what physicians must do to comply," available at: http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/NewPrivacyLegNowInForce.pdf.

[113] See the discussion of the role of Privacy Officers in Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*, July 2003, pp. 13-15.

with using the systems, as well as sanctions for misuse of the system.[114] The importance of such training in a world of electronic health records cannot be underestimated, nor can the ongoing burden of delivering such training effectively be underestimated in a healthcare environment and associated support services where training needs and requirements are already numerous.

Training needs to extend to everyone handling personal health information or accessing the system. This includes IT staff and business staff as well as medical receptionists in physician offices and admitting clerks in hospitals. Medical receptionists and admitting clerks update demographic information, schedule appointments, direct patients with lab test requisitions to appropriate specimen collection centres where necessary, retrieve lab test results and distribute them to physicians in their clinics, and perform other tasks that would make them obvious candidates for access to the EHR Infostructure.[115] In some cases, they also have unrestricted access to the electronic health records of large numbers of patients. It is essential that they understand the privacy rules to be upheld, that their access patterns be monitored and audited, and that there are consequences for breaches of confidentiality. Since many healthcare workers in Canada are unionized, unions have a vital role to play in ensuring that their members understand the privacy and data protection obligations of their members — not least because unions may be representing an employee alleged to be in breach of such obligations.

Resources are available to facilitate privacy training. For example, the BC government has a set of 28 slides that present the basics of BC PIPA.[116] Ontario's Smart Systems for Health (SSHA) has online privacy training for Ontario's PHIPA.[117] Many health information custodians and trustees have also developed their own privacy training geared to the specific interests and concerns of their staff. Some hospitals require physicians and interns to undergo privacy training as a component of the renewal of hospital credentials for these healthcare providers.

5.6 Security Awareness Training

Breaches of privacy are often related to failures in information security. These, in turn, are often traced to users or system administrators who did not understand, or did not follow established security-related procedures. As with privacy, maintaining security requires that everyone working with personal health information and EHR systems have access to continued guidance as security issues arise.[118] Like privacy training, the importance of security awareness training — and the burden of delivering it — cannot be underestimated.

As well as providing basic training in topics such as password protection, security awareness training includes informing users of their responsibilities to report suspected security problems or incidents. Such reports are a first-line defence against software and system errors which can lead to security weaknesses that might otherwise go undetected.

---

[114] On the desirability, and nature of, privacy training, see Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*, July 2003, p. 16.

[115] Canada Health Infoway, "Electronic Health Record (EHR) Privacy and Security Conceptual Architecture," June 2005, p. 51.

[116] See http://www.mser.gov.bc.ca/privacyaccess/Privacy/psp_trainSlides.pdf

[117] http://www.sshaprivacy.com/en/TrainingCentre_Online.aspx

[118] On the desirability, and nature of, privacy training, see Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals,* July 2003, p. 16.

5.7 Information and Guidance for Stakeholders

A basic premise of information governance for privacy and security is that those who want to ask questions — whether patients, their families, physicians, other healthcare professionals, staff, or the media — need to have reliable sources of guidance. Since such questions are often repetitive in nature, one solution is to place Frequently Asked Questions on the websites of healthcare organizations for use by the general public and on the organization's intranet for personnel at all levels. The early examples of University Health Network in Toronto and the Canadian Institute for Health Information have been widely imitated.

5.8 Confidentiality Agreements and Guidance for Signatories

As part of the due diligence associated with the creation and implementation of privacy management plans, healthcare providers and organizations should require all of their staff, including physicians, nurses, staff, researchers, consultants, contractors and students, to sign a confidentiality agreement.[119] Brief, concise, meaningful confidentiality agreements, written in plain language supplemented by “Frequently Asked Questions,” help ensure that staff understand their responsibilities as well as the implications and sanctions that could be imposed for failing to uphold policies and their responsibilities. They are a key component of a data protection regime for many healthcare organizations.[120]

Since much of the data flowing into and out of hospitals involves referrals from the offices of physicians, it is crucial for a hospital to include them in understanding their data protection management plans. The BC Medical Association, for example, has prepared a model confidentiality agreement for employees of a medical practice and for third-party service providers.[121]

5.9 Monitoring Compliance

It is not enough to have best practices for protecting electronic health records from unauthorized access; compliance should be monitored. The objective is to avoid privacy breaches to the fullest extent possible by technical and other means in order to assure trust in the handling of personal health information. These methodologies include real-time auditing and role-based access controls, as discussed elsewhere in this paper.

5.10 Privacy Audit Mechanisms and Site Visits

All health information custodians should have audit logs in place for monitoring access to EHR systems.[122] These need to be monitored on a regular basis and not just in response to an

[119] See Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals,* July 2003, p. 28.

[120] See the sample confidentiality agreement in COACH, *Guidelines for the Protection of Health Information,* p. 86.

[121] See: http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/ConfidentialityEmployees.pdf; and http://www.bcma.org/public/news_publications/publications/PrivacyToolkit/Confidentiality_ServiceProvider.pdf.

[122] For suggestions about audit trails for physicians keeping electronic health records, see Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals,* July 2003, p. 109.

incident. The ability to audit transactions and events taking place within the EHR Infostructure is fundamental to meeting privacy and security requirements. The ability to report on the systems, end-users, patients, and health data involved in each EHR transaction serves a fundamental privacy principle.[123]

Regular audits for compliance need to involve both internal IT auditors and external privacy specialists. A privacy audit has goals and approaches that are similar to a financial audit. As one component of an audit, a privacy specialist should also do site visits to organizations providing outsourced services to observe what is happening in practice with respect to the protection of personal health information.[124] Repeated site visits are excellent awareness-raising exercises about privacy and security requirements.

5.11 Security Audit Mechanisms: Security Vulnerability Assessments and Penetration Testing

Security vulnerability assessments are often carried out on large, operational IT systems to evaluate their security posture. Such reviews are often of a highly technical nature and may rely in part on automated toolsets that test various commercial software components and networks by scanning them for known vulnerabilities.

Penetration testing is typically performed by a third party specializing in this type of security audit. It consists of so-called "ethical hackers" using their expertise to attempt to break into an operational system to gain access to information or to make innocuous, but telling, modifications to system parameters or data. Like vulnerability assessments, penetration testing can take various forms. So-called "black-box" penetration testing provides the testers with no prior knowledge of the infrastructure to be tested, whereas "white-box" penetration testing is conducted after testers are given extensive knowledge of the infrastructure to be tested.

5.12 Memoranda of Understanding

A Memorandum of Understanding (MOU) is a standard way for partners in an information handling activity to set out their respective legal obligations on a variety of matters, including the need to meet legal requirements for data protection and security. An example is the management of a shared digital imaging service among eight hospitals in the Thames Valley region of Ontario, each of which has PHIPA obligations in its own right. These hospitals share an agreement on the collective management of privacy and security obligations, such as access controls and auditing, especially within the context of a shared EHR for the region.

5.13 Contract Language on Privacy and Data Protection Obligations

As noted previously, everyone having access to personal health information in a healthcare setting needs to understand their privacy obligations. Thus, a standard contract between, for example, a hospital and an IT vendor should contain confidentiality language to ensure that the privacy of personal health information will be maintained. BC’s PIPA, for example, requires that

---

[123] Canada Health Infoway, *Electronic Health Record Infostructure Privacy and Security Conceptual Architecture,* Version 1.1, June 2005, p. 108.

[124] See the discussion of both site visits and auditing in Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals,* July 2003, pp. 32-34 and 39-40.

contracts between a service provider, contractor, or consultant and a physician contain contractual language to ensure data protection.[125]

Examples of the types of privacy protective clauses currently found in third-party agreements include:

- **Restriction on agents** (or "affiliates" as they are referred to in Alberta's HIA)**:** Where applicable, agents or affiliates should agree to and acknowledge that they are acting as an "agent" or "affiliate" within the meaning of the applicable privacy statute. As such, they are prohibited from collecting, using, disclosing, retaining, or disposing of data on behalf of any trustee or health information custodian without the custodian's permission. For example, in Ontario, this means that the health information custodian must either have the requisite patient consent or can benefit from an exemption from consent under PHIPA before permitting its agents to deal with personal heath information on its behalf.

- **General limitations:** To limit access to personal health information by third parties as well as internal staff to a need-to-know basis and restrict the collection, use, or disclosure of personal health information to the stated purpose or as required or permitted under the relevant privacy statute.

- **Notification requirement:** To notify the healthcare custodian of any privacy breaches. In Ontario, for example, custodians and their agents must notify, at first reasonable opportunity, when personal health information is lost, stolen, accessed, used, disclosed, copied, modified, or disposed of by unauthorized persons and/or in an unauthorized manner.

- **Privacy requirements:** To protect personal health information using security measures appropriate to the sensitivity of the information and to periodically review and report to the healthcare custodian on the effectiveness of such security measures; to meet or exceed the level of data protection required of the healthcare custodian as per the applicable provisions in any of the privacy statutes.

- **Inspection, Audit and Enforcement:** To permit the healthcare provider to audit and inspect for privacy compliance. The contract should also be made enforceable against a service provider located outside Canadian borders in order to address inter-jurisdictional contraventions.

- **Inquiries and Complaints:** To promptly report to, and co-operate with, health information custodians and trustees if there is any inquiry, complaint or investigation; whether by an individual or the Information and Privacy Commissioner.

- **Liability and Sanctions:** Breach of agreement could result in disciplinary action as well as termination of contract.

As noted in Chapter 2, many third-party agreements are strictly local or regional in nature and were not designed to accommodate information flows across jurisdictional borders. In future, as personal health information flows across jurisdictional boundaries, broader and more comprehensive third-party agreements with vendors and service providers will be needed to

[125] The BC government has model contract language in PIPA Implementation Tool No. 9 at http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/PIPA_Tool_9.pdf.

ensure that accountability is maintained. Healthcare administrators may be able to build on the privacy protective clauses listed above, which at least provide a starting point for outlining governance roles and responsibilities.[126]

5.14 Data Sharing Agreements

A key goal of a data protection policy is to create a "chain of accountability" for identifiable personal information that is leaving, even temporarily, the custody and control of a healthcare organization, including physician offices. Data-sharing agreements can be used to achieve this. The relevant privacy rule is that "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. Contractual or other means can be used to provide a comparable level of protection while the information is being processed by a third-party."[127] Ensuring data-sharing agreements are in place is even more important when an organization is actually disclosing identifiable personal information to an outside party. Depending on the sensitivity of the data transfer, these agreements can be general or specific in nature.[128]

Although provinces with health sector specific laws permit healthcare organizations to share personal health information under the circumstances set out in these statutes and their corresponding regulations, data-sharing agreements are an illustration of a privacy best practice. For example, Ontario's Information and Privacy Commissioner believes that any sharing of personal information should be supported by a written agreement to clarify the rights and obligations of all parties to ensure compliance with relevant legislation. Accordingly, the Commission provides a "Model Data Sharing Agreement," available at www.ipc.on.ca, which includes provisions related to proper data-sharing, retention and disposal of personal information by parties to such an agreement.

5.15 Acceptable Use Agreements

One of the most important means for ensuring that end-users are aware of their responsibility for appropriate access and use of patient data and, furthermore, in protecting the confidentiality of the information, is to have each user sign an acceptable use agreement prior to gaining access to the EHR for the first time.

Some acceptable use agreements are supplemented by a brief statement presented online that users must acknowledge each time they log into the system by clicking a button marked "I agree." The latter is a useful tool in reminding users of their responsibilities but is no substitute for a signed written agreement. Such written agreements can form the basis of legal action against users who flout the provisions of the agreement.

---

[126] See Chapter 3 for a discussion of the privacy protective clauses used in the context of a master service level agreement between Cancer Care Ontario and a US service provider

[127] PIPEDA, Schedule 1, 4.1.3.

[128] See Ontario Hospital Association, *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*, July 2003, pp. 31-32 for specific examples of such data transfers as well as suggested contents for a data sharing agreement (pp. 64-66).

6. LESSONS FROM OTHER JURISDICTIONS AND OTHER INDUSTRIAL SECTORS

Canada is one of a handful of countries devoting significant resources to the building of a comprehensive EHR. Lessons can be learned from similar developments currently underway in the UK, Australia, Japan and the US. In particular, the UK Department of Health has been grappling with information governance issues since 2001 and some of the work done by the UK National Health Service (NHS) merits attention by those involved in similar work in Canada. This chapter briefly examines this and other work from healthcare jurisdictions outside of Canada.

There are also lessons to be learned from other industrial sectors that have built large-scale, complex information infrastructures and so we also examine some of the relevant developments that have taken place in Canada and elsewhere in information governance outside of health care.

6.1 Lessons Learned from Other Jurisdictions

UK National Health Service (NHS) Information Governance Toolkit

The NHS defines information governance as "a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service." The NHS sets information handling standards and gives organizations the tools to achieve these standards in five areas:

1 **Holding** information securely and confidentially;

2 **Obtaining** information fairly and efficiently;

3 **Recording** information accurately and reliably;

4 **Using** information effectively and ethically; and

5 **Sharing** information appropriately and lawfully.

In 2001, the NHS provided an assessment toolkit for information security measures undertaken by English hospitals. The toolkit measured assessment against the ISO 17799 security standard (*Information Technology – Code of Practice for Information Security Management*). The toolkit included a program to assist hospitals with formulating a security policy by guiding a user through a pre-programmed question and answer session. The success of this undertaking led the UK Department of Health to develop a broader information governance toolkit that included both privacy and security. The current version of this information governance toolkit takes the form of a detailed spreadsheet with pre-programmed macros that automatically calculate scores and graphical presentations of the breadth and comprehensiveness of the hospital's information governance practices.

While this approach involves self-assessment (the “hospital trust”, as it is called, is responsible for providing its own responses to the questions posed by the toolkit), a written statement must accompany each answer stating what evidence is available to support the answer given. The results of the assessment are carefully reviewed and hospitals are rated on their responses. After several years of use and refinement, hospitals now work hard to improve below-average scores and aspects of the assessment are made available to interested members of the public.

The toolkit's questions are divided into a number of categories: healthcare records management, clinical information assurance, confidentiality and data protection assurance, secondary uses, freedom of information, information governance management, and information security assurance. Answers place the hospital into one of several attainment levels for each question. An example of one of the 23 questions from the data protection category is the following:

> *Does the Organization ensure that it has formal contractual arrangements that include compliance with information governance requirements, with all contractors and support organizations?*

Answer choices are as follows:

- The Organization does not include Service User confidentiality, security and data protection requirements in contracts with contractors and support organizations (attainment level zero).
- At a minimum, basic agreements of undertaking should be signed by contractors to draw their attention to Service User confidentiality, security and data protection requirements (attainment level one). Supporting evidence for this answer would include examples of signed agreements.
- The Organization ensures that all formal contracts include appropriate Service User confidentiality, information security and data protection requirements (attainment level two). Supporting evidence for this answer would include examples of signed agreements.
- The Organization ensures that formal contracts with appropriate information governance requirements are in place with all contractors and support organizations (attainment level three). Supporting evidence for this answer would include details of all contracts.

The toolkit also includes suggested improvement plans for attaining a higher level and a maintenance plan if the hospital has attained the highest level for this question.

The Department of Health has created a version of the toolkit for primary care practices and plans to begin assessing them in the near future.

While not all the questions and answers in the NHS information governance toolkit would be directly applicable to Canadian healthcare institutions, many probably could be and others could be modified to make them relevant within a Canadian context. Any stakeholder wanting to develop evaluative tools to assess the state of information governance in a Canadian jurisdiction would do well to take the NHS toolkit. Further information can be found at https://www.igt.connectingforhealth.nhs.uk/

Santa Barbara County Care Data Exchange

In introducing the information governance toolkit discussed above, the NHS had an enormous advantage in being directly responsible for the funding of all hospitals and primary care trusts (as they are called in the UK) in England. But can an overarching information governance structure work in a cooperative fashion when stakeholders are not tied to a single funding source? The Santa Barbara County Care Data Exchange, in California, was an example of such an arrangement. It operated from 1998 until early 2007.[129]

The Exchange was organized as a non-profit “loosely coupled” utility for securely exchanging clinical information. It was available to anyone who chose to join. A partnership model was chosen to minimize up-front, inter-organizational legal risks. The initial project was supported by a $10M US grant from the California Healthcare Foundation, which also provided funds to support IT systems purchases by individual organizations participating in the Exchange. Investment from local healthcare organizations was expected to fully fund ongoing operations,

The information governance of the Exchange was in the hands of a Care Data Exchange Council that provided overall governance and was composed of one senior leader from each participating organization; each received one vote on all decisions. The Council determined business and operating policies, addressed legal and business issues, and set priorities. Technical Advisory and Clinical Advisory Committees reported to the Council. Security and privacy practices fell under the mandate of both of these committees. Four Care Data Alliances made up of public and private stakeholders across Santa Barbara County reported to the Council and were bound by user agreements. These user agreements included HIPAA-consistent data use and disclosure requirements that were compliant with the US Health Insurance Portability and Accountability Act, 1996 (HIPAA). Substantial effort and financial resources were put into legal reviews to address US federal and California state privacy laws.

Stringent security specifications were built into the technology design and implementation (authentication, informed consent, auditing, and logging) and strict access control policies were in place. The Exchange believed the most important components of security to be the business processes surrounding it, so care was taken to ensure that complaints and access control procedures were handled expeditiously.

Several information governance lessons were learned over the more than eight years in which the Exchange operated. Physician concerns were raised about whether the clinical data exchanged could be pooled and used to profile or evaluate their practices. As a result, assurances were put in place that this would not happen. There was also user resistance to security certificates and requests for other forms of authentication.

There appears to be a first-mover disadvantage in making health information interoperable due to intra-organizational barriers that are compounded in a regional context. Health information exchange is likely to remain incremental despite the technological ability to enable it.

The need for independent and locally trusted third parties to act as catalysts in the development of health information exchange efforts has been compelling. The now defunct Exchange stated that the success of regional health information exchange efforts is tied to the extent to which they are locally driven; building on existing care delivery systems and trust relationships.

[129] Effective March 2007, the Santa Barbara County Care Data Exchange ceased operation. In the article “*What Killed the Santa Barbara County Care Data Exchange?”* Bruce Merlin Fried, Esq. March 12, 2007 explains that although privacy and security concerns were mostly overcome, there remained significant outstanding hurdles such as, challenges in technical interfaces with legacy systems, liability issues, lack of an on-going funding model and lengthy delays in full deployment. The article is available at http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemid=131621

Kaiser Permanente

Kaiser Permanente is the largest non-profit health plan in the United States and serves the health care needs of 8.2 million patients in nine states and the District of Columbia. It was founded in 1945 as a non-profit, group-practice health plan with headquarters in Oakland, California. Today, it encompasses Kaiser Foundation Health Plan, Inc. (a non-profit, public-benefit corporation), Kaiser Foundation Hospitals (a non-profit, public-benefit corporation), and the Permanente Medical Groups (for-profit professional organizations), as well as Permanente Dental Associates. As of 2003, Kaiser had 135,000 employees and 11,000 physicians.

The Kaiser Permanente HealthConnect program functions as an interoperable EHR across Kaiser Permanente. It is currently the world's largest deployment of an EHR. It integrates clinical records with appointments, registration and billing: A patient's medical history is available to every clinician who is involved in that patient's care, even if the primary care physician is in Georgia, an attending nurse is in Colorado, and a consulting specialist is in California. It also includes features such as maintenance of a medication profile for patients and checking for drug interactions when new prescriptions are entered. Patients now have access to portions of their record online, as well as being able to book appointments online. Security features include role-based access control: Mental and behavioural health specialists can see mental health records, but other health professionals will only gain access to the information in emergencies. Indeed, the size, scope and sophistication of Kaiser's EHR mirror many aspects of the interoperable EHR envisioned by *Infoway*.

In 1997, the Permanente Federation, a limited liability company, was created as a partnership among the Permanente Medical Groups. This partnership entrusts the Federation with national decision-making authority for the regional Permanente Medical Groups. The Federation is governed by a five-person executive committee made up of four executive medical directors and an appointed executive director who is responsible for day-to-day activities.

Accountability is demanded of Kaiser's system users: All are held personally accountable for protecting patient data. This accountability is enforced through routine surveillance and investigation of complaints using audit records of accesses and actions. Sanctions include termination of employment and notification to appropriate authorities

Kaiser explicitly describes "rights" to which its participating members (i.e., patients) are entitled. They include privacy rights such as a guarantee not to release medical information without express patient consent or as required or permitted by law, the right to receive copies of medical records, the opportunity to correct mistakes, and the right to receive an accounting of who has accessed a patient's record. As providers of health care and health plans, Kaiser is subject to oversight conducted by federal and state agencies. These agencies may conduct audits of operations and activities. Kaiser is subject to HIPAA and certain state laws on privacy.

More information is available at
http://members.kaiserpermanente.org/kpweb/historykp/entrypage.do and
http://www.himss.org/handouts/SafeguardingPrivacy-October10.pdf

6.2 Lessons Learned from Other Industrial Sectors

Interac Association

Interac develops and operates Canada’s national network of two shared electronic financial services: Shared Cash Dispensing at automated banking machines (ABMs) and Interac Direct

Payment (IDP, national debit service). In 2003, there were 35,000 ABMs available in Canada, and two billion purchases made using IDP. The network is completely decentralized so there is no single point-of-failure that might shut the system down.

Interac is an unincorporated, non-profit association. The association exists to facilitate the exchange of settlement obligations between a cardholder's financial institution and the operator of the terminal; it plays no part in the actual transfer of funds. Membership includes banks and other financial institutions, but any company incorporated in Canada is eligible to join. The Interac Association collects fees to cover operating costs from its members, not from cardholders.

A 14- member Board of Directors oversees all aspects of governance. It is composed of member-appointed representatives in proportion to transaction volumes. The Board sets and enforces the rules governing transactions routed over the Inter-Member Network, and oversees management of network operations, common marketing support and promotion of Interac services.

The Association endorses the Canadian Code of Practice for Consumer Debit Card Services (prepared by the Electronic Funds Transfer Working Group) which was developed to help protect consumers in their use of debit card services in Canada by clarifying consumer and industry responsibilities. The Code outlines standards regarding cardholder agreements and consumer disclosure, liability for loss and dispute resolution.

The Interac experience shows that a large-scale, Canada-wide IT network can be efficiently deployed and governed to enable highly reliable, high-volume exchanges of confidential personal information among a diverse set of stakeholders.

More information is available at www.interac.org

Canadian Securities Administrators (CSA)

The CSA is a forum for the 13 securities regulatory authorities of Canada's provinces and territories to coordinate and harmonize regulation of Canadian capital markets; as well as to share ideas, design policies and regulations that are consistent across the country, and ensure the smooth operation of Canada's securities industry. It is a cooperative membership association. Funding and support are provided on a voluntary basis from each member's operating budget.

Certain activities are fundamental to each provincial or territorial regulator: reviewing prospectuses; monitoring continuous disclosure documents; conducting compliance reviews of registrants; granting discretionary exemptions from regulatory requirements; educating and informing industry and investors; conducting investigations of possible violations of securities laws; and commencing proceedings before a tribunal or applicable Provincial Court of Justice. As in health care, securities administrators must deal with jurisdictional variances in regulations. Despite these variances, the CSA has determined a core set of regulatory requirements that are substantially the same in all jurisdictions and are of fundamental benefit to investors and capital markets. The CSA works toward regulatory initiatives that are coordinated across the country, as its members believe these best serve investors and markets. CSA members also believe regulation must accommodate both national and local concerns, priorities and issues.

The CSA was re-structured in September 2003 into a more formal organization. A Chair and Vice-Chair are elected by members for two-year terms. A permanent Secretariat opened in

March 2004 in Montreal. It provides the organizational stability necessary for CSA to function efficiently. A Policy Coordination Committee (an executive-style committee to oversee CSA's policy initiatives) was established in August 2003. Its members are the chairs of six regulators (BC, Alberta, Manitoba, Ontario, Quebec, and Nova Scotia). Each CSA member has its own staff that works on policy development and delivers regulatory programs through their participation in CSA Committees. Among the standing committees of the CSA is one devoted to information systems.

The CSA also has a standing committee on enforcement that shares information and identifies gaps and trends in enforcement activities. The committee focuses on the inter-relationship and interplay between the various national and international organizations, agencies and self-regulatory organizations involved in the detection, investigation and prosecution of illegal market activities. It identifies Commission and Court decisions which might have an impact on the regulatory regime and implements the consequent policies. It establishes and maintains cross-jurisdictional processes and coordinated inter-jurisdictional investigations. It also maintains a database of enforcement activity.

Those readers concerned about the effect that inter-jurisdictional data transfers may have on health information custodial responsibilities may find the CSA's approach of interest. The CSA has developed a system of "mutual reliance" that designates one securities regulator as the lead agency when it comes to reviewing applications or disclosure documents from companies which report to more than one jurisdiction. A Mutual Reliance Review System (MRRS) was introduced in 1998 to reduce unnecessary duplication in the review of filings made in multiple jurisdictions. The purpose of this system is to increase market efficiency by streamlining the process and reducing the number of regulatory agencies a company must deal with. It was implemented through a Memorandum of Understanding among the CSA members, based on the principles of mutual reliance. Mutual reliance means that, in exercising discretion under securities legislation, the decision-maker in a particular securities regulatory authority is prepared to rely primarily on the analysis and review of the staff of another securities regulatory authority. The MOU does not involve a delegation of power by the various securities commissions. Jurisdictions “opt in” to a principal regulator’s decision and “opt-outs” must be reported quarterly to CSA Chairs. There are very few opt-outs under this scheme. Mutual reliance principles are also applied to effect streamlined regulation in other contexts such as enforcement and registrant regulation.

Clearly, the CSA has surmounted challenges posed by jurisdiction-specific securities laws and regulations and has worked out common requirements. By adopting the Memoranda of Understanding described above, members have streamlined inter-jurisdictional transactions in the face of differing jurisdictional securities legislation and regulation. Perhaps a similar effort among healthcare jurisdictions in Canada would likewise be successful in dealing with the cross-jurisdictional handling of important issues such as consent, security incident handling and privacy breaches.

Australian Standard on IT Information Governance

Australia has produced a standard on information governance. Australian standard AS 8015-2005 *Corporate Governance of Information and Communication Technology* provides a framework of principles for governance boards of organizations to use when evaluating, directing and monitoring the IT portfolio of the organization. It is related to another Australian standard, AS 8000-2003 *Corporate Governance – Good Governance Principles*, that provides guidance on good governance principles and codes of conduct.

The purpose of the first standard is threefold:

- To promote effective, efficient and acceptable use of ICT in organizations by providing stakeholders (including consumers, shareholders, and employees) with the confidence that, if the Standard is followed, they can trust in the organization's corporate governance of ICT;
- Informing and guiding Directors of organizations in governing the use of ICT in their organization; and
- Providing a basis for objective evaluation of the corporate governance of ICT.

The standard lays out six principles for good information governance related to establishing clearly understood responsibilities, planning, acquisition, performance, conformance and respect for human factors. It also provides a model that directors of organizations can follow that involves three tasks: evaluating the use of ICT; preparation and implementation of plans and policies; and monitoring conformance to policies, and performance against the plans. A framework is included that guides implementers of the standard on how best to implement each of the six principles.

The second standard on corporate governance discusses structural elements of good governance, such as commitment, governance policy, board responsibility, continuous improvement; operational elements of governance, such as identification of issues, operating procedures for governance, dealing with breaches and complaints, and record keeping; and maintenance elements of good governance, such as education and training, communication, monitoring, assessment and review, and liaisons. It also lays out governing board responsibilities, disclosure and transparency obligations, and the roles of stakeholders in governance, among others.

While no similar Canadian standards exist yet, these Australian standards are a good starting point for the elucidation of information governance principles.

International Air Transport Association (IATA)

IATA is the primary vehicle for inter-airline cooperation in promoting safe, reliable, secure and economical air services. It is a non-profit, membership-based, global trade association representing 270 members from more than 140 nations and 94 per cent of international scheduled air traffic. Its members are all airlines, but other industry partners (suppliers, travel agencies, and freight forwarders) can participate as non-members in different IATA programs and benefit from operational resources. IATA's budget is paid by dues collected from members.

IATA's mission is to represent and serve the airline industry while:

- Promoting safe, reliable and secure air services;
- Providing means of collaboration among airlines engaged in international air transport; and
- Cooperating with the International Civil Aviation Organization and other relevant international organisations.

The Board of Governors exercises executive committee functions and is accountable to the Association's annual General Meeting, at which members have the opportunity to vote and make final decisions on all matters. The Board of Governors acts on behalf of, and in the interests of, the Association. In this capacity, its members represent the Association as a whole. The Board is composed of not more than 31 persons elected for a three-year term from among representatives of active members, who serve without remuneration.

IATA has a six-point safety and security program:

1. Safety auditing (the first airline safety audit program based on internationally harmonized standards; designed to help airlines share audit resources and reduce the overall number of audits performed);
2. Infrastructure safety (e.g. air traffic control, pilot/controller);
3. Safety data management and analysis (i.e., event monitoring and occurrence investigation support);
4. Safety management systems (sets out a company's safety policy and its intent to manage risk);
5. Flying operations; and
6. Cargo and dangerous goods safety.

The safety and security of airlines systems are no less critical than those in health care. IATA has surmounted legal, regulatory, operational and practical barriers to promote the smooth interoperation of sophisticated mission-critical IT systems that span 140 countries. This was achieved cooperatively in spite of IATA's members being business rivals in the highly competitive airline industry. In contrast, a pan-Canadian interoperable EHR would operate within many fewer jurisdictions and perhaps connect to fewer interoperating systems. Those involved in implementing the pan-Canadian EHR can draw inspiration from the success of undertakings such as the one described above.

7. CONCLUSIONS

Conclusions

The overall objectives of the pan-Canadian interoperable EHR initiative are to increase the efficiency of the health system, improve access to health services and improve the quality of health services provided to Canadians. This will be achieved in part by increasing the speed and volume at which authorized end-users share and/or transfer patient information.

Governance is not a new concept and information governance is not new to the health record environment. Many components of information governance discussed in this paper apply and have been addressed to varying degrees in the paper world of health records. However, the interoperable EHR changes the environment within which information flows. As such, the rules related to information collection, use, disclosure and management in an interoperable EHR environment bear careful consideration, especially if EHR initiatives are to be accepted by healthcare providers and the public.

With respect to the vast array of information governance topics identified in this paper, the large number of diverse stakeholders with interest in these topics, and the complex legislative, regulatory and ethical schema that must be respected, it is likely that a variety of approaches to information governance will be required. These options could involve cross-disciplinary committees, or intra-jurisdictional working groups or teams, among others, to identify and arrive at information governance solutions for a pan-Canadian interoperable EHR.

Consideration also needs to be given to where responsibility for information governance management will reside. Perhaps it can be managed from within existing information governance structures, or perhaps, similar to Interac, the Canadian Securities Administrators and the International Air Transport Association, an additional central structure will be necessary in order to be seen to provide an effective and efficient way to manage some of the information governance topics identified in this paper.

Information governance in the interoperable EHR is already beginning to be addressed and considered by many involved in the EHR initiative. It is recognized that it will take time to involve the necessary stakeholders and arrive at acceptable approaches. Currently, EHR developments are primarily domain and jurisdiction based and it will be some time before interoperability is achieved within a jurisdiction, let alone at a pan-Canadian level. As such, while some topics, such as role-based access, may require attention in the short term, in other cases there is time to address the topics in an incremental manner, over time, on an intra-jurisdictional basis as the components of interoperable EHR systems develop and as the information necessary to arrive at reasonable approaches becomes available. Further, as noted in the paper, there are many information governance mechanisms currently in place that apply to the world of paper-based records, which can be leveraged for the development of future information governance solutions in a pan-Canadian interoperable EHR environment.

This paper is intended to foster discussion and promote action. Readers are encouraged to share this paper with their colleagues.

Infoway also remains committed to exploring these topics and to this end will be meeting with stakeholders during the winter of 2007. Comments can also be submitted directly to:

Joan Roch, Chief Privacy Strategist
Canada Health Infoway
1000 Sherbrooke Street West, Suite 1200
Montreal, Quebec H3A 3G4

Tel: (514) 237-0521
Fax: (514) 221-2258
Email: jroch@infoway-inforoute.ca

APPENDIX: SOURCES OF INFORMATION

Works Cited

Advisory Committee on Information and Emerging Technologies (ACIET), *Pan-Canadian Health Information Privacy and Confidentiality Framework*, Ottawa: Health and the Information Highway Division, Health Canada, January 2005. Available at http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html.

Alberta Netcare. *Alberta Physician Office Program*, June 2006; available at: http://www.posp.ab.ca/

Ball, Ted, Dennis Pointer, and Liz Verlaan-Cole. "Governance and Management roles in Transforming and Integrating Independent Organizations within Interdependent Local Networks". *Law and Governance* 8.10 (2004).

Brailer, David, et al. *Moving Toward Electronic Health Information Exchange: Interim Report on the Santa Barbara County Data Exchange*. Oakland, CA: California health care Foundation, 2003.

Brunelle, Fran, Peggy Leatt, and Sandra Leggat. "Health care Governance in Transition: From Hospital Boards to System Boards…A National Survey of Chairs of Boards". *Hospital Quarterly* Winter (1998/1999): 28-34.

Canada Health Infoway. *Governance of an Interoperable EHR: Issues for Consideration.* 15 July 2005. Powerpoint presentation.

Canada Health Infoway. *Electronic Health Record Privacy and Security Requirements,* 2005.

Canada Health Infoway. Electronic Health Record Privacy and Security Use Cases, 2004

Canada Health Infoway. *Electronic Health Record Privacy and Security Conceptual Architecture,* 2005.
Available at http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf

Canada Health Infoway. *Electronic Health Record (EHR) Privacy and Security Requirements, version 1.1,* 2005.
Available at http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf

Canada Health Infoway. *The Electronic Health Record Solution Blueprint: A Roadmap for Planning and Implementation in Canada*. 2003, revised 2006.

Canadian Securities Administrators (CSA). *Strategic Objectives*. Montreal: CSA, 2005.

Canadian Securities Administrators (CSA). Introduction to the Canadian Securities Administrators. Montreal, CSA, 2006.

Clark, Woodrow W, and Istemi Demirag. "Enron: The Failure of Corporate Governance".
JCC 8 (2002): 105.

COACH, Guidelines for the Protection of Personal Health Information,
Available at www.coachorg.com
College of Physicians and Surgeons of Alberta, Medical Informatics Committee, *Data Stewardship Framework, version 1.2,* December 2006. Available at:
http://www.cpsa.ab.ca/publicationsresources/attachments_other/CPSA_Data_Stewardship_Framework.pdf.

Committee on the Financial Aspects of Corporate Governance. *Report*. Adrian Cadbury (Chair). 1 December 1992.

Cross, Michael. "Patients, not the State, Own Medical Records, says GP". *The Guardian (UK)* 6 July 2006.

Department of the Taoiseach. *Regulating Better: a Government White Paper Setting Out Six Principles of Better Regulation.* Dublin Department of the Taoiseach, 2004.

Edgar, Laura. *Building Policy Partnerships: Making Network Governance Work.* Ottawa: Institute on Governance, 2002.

Ellsmore, Nick. *Privacy and Security: Corporate Governance Issues for Business.* Sydney: SIFT Pty Ltd, 2002.

Elson, Steve. The Evolution of Health System Governance in Canada and Ontario. *Law and Governance* 10.2 (2006).

Entrust. *Information Security Governance (ISG): an Essential Element of Corporate Governance.* Addison, Texas: Entrust, 2004.

Gill, Mel. *Governance Do's and Don'ts: Lessons from Case Studies on Twenty Canadian Non-Profits.* Ottawa: Institute on Governance, 2001.
Available at http://www.iog.ca/publications/nonprofit-gov.PDF

Government of Alberta, *Frequently Asked Questions: Alberta's Electronic Health Record.* Available at
http://www.health.gov.ab.ca/resources/publications/QAs.pdf#search=%22EHR%20masking%22

Graham, John, Bruce Amos, and Tim Plumptre. *Principles for Good Governance in the 21st Century. Policy Brief No. 15.* Ottawa: Institute on Governance, 2003.

Standing Senate Committee on Social Affairs, Science and Technology. Michael J.L. Kirby (Chair). *The Health of Canadians: the Federal Role. Final Report. Volume Six: Recommendations for Reform.* Ottawa: The Senate, 2002. Chapter 1, Section 1.2.

Interac Association. *Interac Association: A Backgrounder.* Toronto, 2003.

International Organisation for Standardisation (ISO), *ISO 17799:2005: Information Technology – Code of Practice for Information Security Management*

IT Governance Institute. *Board Briefing on IT Governance*. 2nd ed., 2003.

IT Governance Institute. *IT Governance Executive Summary,* IT Governance Institute. *Information Security Governance: Guidance for Boards of Directors and Executive Management*. 2nd ed., 2006.

Marchibroda, Janet, and Jennifer Covich Borderick. *Emerging Trends and Issues in Health Information Exchange. Second Annual Survey of State, Regional, and Community-Based Health Information Exchange Initiatives and Organizations.* Washington, DC: eHealth Initiative Foundation, 2005.

Markle Foundation. Connecting for Health Steering Group. *An Overview of the Connecting for Health Common Framework.* New York, NY: 2006.

Organization for Economic Co-Operation and Development. *OECD Principles of Corporate Governance*. OECD, 2004.

Power, E. Michael and Roland L. Trope. *Sailing in Dangerous Waters: a Director's Guide to Data Governance*. Chicago: American Bar Association, 2005.

Rowland, Christopher. "Digital Files Raise Security Concerns: Questions Posed About Patient Computer Data". *The Boston Globe*
26 June 2006.

Saskatchewan Health. Enterprise Architecture: An Examination of the Characteristics of an "Enterprise Client Identifier." White Paper: Health Information Solutions Centre, 2005.

Sheffield Teaching Hospitals. *Information Governance Policy.* Sheffield: NHS Foundation Trust, 2005.

Standards Australia International. *Corporate Governance of Information and Communication Technology.* AS 8015-2005, Sydney: Standards Australia, 2005.

Standards Australia International. *Good Governance Principles.* Sydney: Standards Australia, 2004.

The Good European Health Record. *Description of the GEHR Architecture*, June 2006. Available at http://www.chime.ucl.ac.uk/work-areas/ehrs/GEHR/GEHRdesarchitecture.htm